Universiteit Antwerpen

ICT Code of Conduct for students

Universiteit Antwerpen

Table of contents

1 Introduction 3
2 Definitions 4
3 Purpose and scope 5
4 General principles 6
4.1 Authorised usage 6
4.2 Unauthorised usage 6
4.3 Personal usage 6
5 Information management and security 7
5.1 Security 7
5.2 Storing, sharing or copying company data 7
5.3 Personal data 7
5.4 Cloud 7
5.5 Access rights 7
6 ICT systems 9
6.1 General 9
6.2 ICT systems of the University of Antwerp 9
6.3 External ICT systems 10
6.4 Accounts and passwords 10
7 Communication 11
7.1 E-mail 11
7.2 Internet 11
7.3 Telephony 11
8 Obligation to report 12
8.1 Incidents 12
8.2 Incidents with personal data 12
9 Supervision and control 13
10 Measures in the event of infringement 14
11 Exemptions 15

1 Introduction

Information and communication technology (ICT) is playing an increasingly important role in society and thus also within the University of Antwerp. The proper functioning of the university is therefore increasingly dependent on the smooth and effective operation of the ICT infrastructure.

However, this smooth and effective functioning of ICT cannot be achieved by technical measures alone. The users of ICT resources must also play their part. This standard provides a general framework of values and principles that the students of the University of Antwerp should respect when using ICT resources related to the University of Antwerp.

The intention of this standard is not to go against the culture of openness, trust and integrity of the University of Antwerp or the principle of academic freedom, but to protect the students, employees, partners and the university from illegal or damaging actions of individuals or groups, known or unknown.

The university encourages all members of the university community to use electronic resources in a respectful manner. Each user therefore has a number of responsibilities associated with the use of ICT resources at the University of Antwerp.

2 Definitions

ICT resources consist of ICT systems (i.e. hardware and software) on the one hand, and the data stored on ICT systems on the other. Examples are: e-mail facilities, accounts, internet, computers, laptops, tablets, printers, USB sticks, telephones, mobile phones, smartphones, storage media (servers etc.), routers, switches, etc. The term **data** (information) includes all meaningful data.

Company data is all meaningful data that is owned by the University of Antwerp. It concerns, for example, data that are subject to intellectual property rights, data that are necessary for the execution of business processes, personal data of staff members and students, etc.

Processing is an operation or set of operations relating to data, whether or not carried out by means of an automated process, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction of data.

Students are all natural persons who are registered in the student database.

3 Purpose and scope

The objective of this standard is:

- To guarantee the security and reliability of ICT resources related to the University of Antwerp and relevant third parties;
- To guarantee a stable ICT service;
- Protect the privacy and security of individual users and;
- Guarantee the good name of the University of Antwerp as a responsible internet user.

This standard applies to each student when using ICT resources that are related to the University of Antwerp (including telephone, GSM, fax, pc, e-mail, network software, internal and external networks, Internet, test and learning platforms, administrative systems, information systems, company data on the ICT systems, etc.).

This standard therefore applies equally to ICT resources, whether or not owned by the University of Antwerp, used in relation to the University of Antwerp (e.g. University of Antwerp email address) or in combination with the ICT resources of the University of Antwerp (e.g. access to Blackboard).

All students are expected to be familiar with these rules and to conduct themselves accordingly.

4 General principles

4.1 Authorised usage

Every student is expected to behave like a good father when dealing with ICT resources related to the University of Antwerp. This principle implies that every student should behave as a normal and careful person with foresight:

- **Foresight** means that one tries to reasonably estimate the adverse consequences of one's actions and, in other words, tries to anticipate them;
- **Careful** means that one tries to avoid those adverse effects by taking appropriate precautions.

4.2 Unauthorised usage

The unauthorised use of ICT resources relating to the University of Antwerp is prohibited. Below is a non-exhaustive list of unauthorised actions:

- Using ICT resources that are related to the University of Antwerp to perform actions or process data (storage, distribution, processing, etc.) that:
    - Are insulting, defamatory, offensive, threatening, discriminating or constitute a breach of trust;
    - May cause damage to third parties;
    - Are contrary to public order and morality;
    - Could harm the image, the moral or economic interests of the University of Antwerp;
    - Contravene legislation and regulations on computer crime, the protection of privacy, intellectual property rights, the protection of trade names, etc. and/or;
    - In conflict with the policy vision and/or internal regulations of the University of Antwerp.

4.3 Personal usage

The University of Antwerp allows the personal use of its ICT resources within reasonable limits. This means that :

- Others should not be disturbed by this use in the exercise of their (professional or study) activities;
- Unless otherwise agreed, no costs are charged to the University of Antwerp and;
- Educational purposes are always given priority in the use of shared ICT resources.

Users who process personal data on ICT resources of the University of Antwerp, should be aware that in exceptional cases the University of Antwerp can take cognizance of the information processed on the ICT resources of the University of Antwerp. In any case, the privacy of the person concerned is protected as much as possible.

The University of Antwerp does not accept any liability for the possible loss of private data, stored on the University of Antwerp's ICT resources.

5 Information management and security

5.1 Security

All (confidential) information must always be protected by appropriate technical and organisational security measures. Students must therefore ensure that confidential information is always stored on systems for which appropriate security measures have been taken (such as anti-virus software, an active firewall, etc.).

In addition, students themselves must always take sufficient security measures to minimise the possibility of hacking into the University's systems and the theft or loss of ICT resources (use of strong passwords, not leaving laptops unattended, not storing passwords on computers (unless they are stored in a password manager and the database is not on a shared computer), etc.).

Students should ensure that confidential company data (such as personal data processed in the context of a thesis) that is stored on portable media (laptop hard drives, USB sticks, etc.) is encrypted. More concrete agreements on the encryption of ICT resources are published on Blackboard.

5.2 Storing, sharing or copying company data

Preferably, company data (such as research data) are stored on systems managed by the ICT department. Storing data on local media (such as external hard disks, the hard disk of a laptop, etc.) should be avoided as much as possible.

If this is not possible, the students involved must ensure that a sufficiently high level of protection is guaranteed for the alternative ICT systems. These protection measures include taking regular backups, using security software and sufficiently strong authentication methods (such as a complex password), encrypting portable media, etc.

It is not permitted to distribute or share company data (such as course material, but also research data) with persons who are not authorised to process these data (receive, consult, distribute, publish, etc.).

5.3 Personal data

Personal data may be processed on the ICT-systems of the University of Antwerp to the extent that this is in accordance with the applicable privacy legislation and the privacy regulations of the University of Antwerp.

For more information on the processing of personal data, please refer to the appropriate communication channels of the Data Protection Authority (e.g. the privacy helpdesk).

5.4 Cloud

Only the cloud applications that have been approved by the ICT Department of the University of Antwerp may be used to store company data (such as course material and research data).

For the storage of personal data in cloud applications, the guidelines of the Privacy Service must always be followed. For more information about the processing of personal data in cloud applications, please refer to the appropriate communication channels of the Data Protection Service (e.g. the privacy helpdesk).

5.5 Access rights

The granting of access rights is exclusively based on the need-to-have and need-to-know principles. In concrete terms, this means that students may only be granted access rights that are necessary in the framework of their

study activities at the University of Antwerp. It is the responsibility of the data owners to make sure that the access rights are correct and limited to what is strictly necessary.

An evaluation of the access rights to the information for which they are responsible should be carried out on a regular basis by the data owners.

If a student notices that he or she has access to information for which he or she is not authorised, the student must report this immediately to the data owner and/or the ICT manager, so that access can be restricted.

The request for obtaining access rights is always made or set by the data owner of the information concerned.

6 ICT systems

6.1 General

It is forbidden to attempt to bypass the security of a host, network or account. This includes, but is not limited to: requesting data that is not intended for the user, using a service or account that the user is not authorised to use, using sniffing and scanning tools, etc.

It is also prohibited to attempt to disrupt any service, host or network (denial of service). This includes, but is not limited to, explicit attempts to overload a network or host (flooding), and attempts to crash a system.

It is not allowed to install own network equipment (switches, routers, firewalls, vpn-servers, dialin-servers, wireless access points, ...) without consultation and explicit permission of the Network Service of the ICT Department.

Students must always ensure that their activities on the network or the systems of the University of Antwerp do not cause damage or inconvenience (of any kind) to other users or third parties.

Students should at all times be cautious when logging on to the University of Antwerp network from other, external (public) locations (e.g. logging on via cybercafés, open/public wireless networks, etc.).

Students must ensure that all software and data obtained via an external network, via web applications (such as webmail, web hosting, etc.) or via portable media (such as CD-ROMs, DVDs, USB sticks, etc.) are checked for viruses and other malicious software.
It is not allowed to store non-professional data on central ICT-systems (such as servers and the central storage) of the University of Antwerp.

It is forbidden to use the network of the University of Antwerp for profit-making or trade purposes, or for activities that are not in line with the mission of the university, or for other activities that are in conflict with the AUP of Belnet.

It is explicitly forbidden for students to carry out illegal downloads (such as software, files, music files, film files, etc.) via or to install them on ICT resources that are related to the University of Antwerp. If a student does not respect this provision, this is the full responsibility of the student. Possible legal investigations and the related financial consequences will always be forwarded to the student concerned.

The University of Antwerp reserves the right to block access to all or part of the network by certain ICT devices (e.g. smartphones, tablets, laptops, etc.) at all times if necessary (e.g. in case of theft, loss, etc.).

6.2 ICT systems of the University of Antwerp

Students have the responsibility to use ICT resources, which are made available, safely.

In order to prevent theft and loss, students must always take sufficient security measures. For example, the screen saver of the ICT-systems should always be activated when the ICT-systems are left unattended.

Students may only install and use software on ICT resources of the UAntwerpen for which the necessary licences or user agreements are in place. It is forbidden to pass on personally obtained user rights and licenses of the University of Antwerp to third parties.

The ICT systems of the University of Antwerp must be equipped with active security software. It is forbidden to disable security and management software (e.g. anti-virus software) installed by the ICT department.

If, despite various security measures, the student is confronted with a virus, a suspicious e-mail or a suspicious file, work on the ICT system must immediately be stopped and these must first be removed. In the above cases, the ICT Department must always be contacted.

6.3 External ICT systems

It is forbidden to connect ICT systems that are not the property of the University of Antwerp and that do not meet the security rules imposed by the internal regulations of the University of Antwerp, to the physical campus network. For example, external ICT systems (such as laptops, tablets, smartphones, etc.) must always have an active firewall and anti-virus software.

The use of one's own ICT systems is at one's own risk. Consequently, students who bring their own external ICT system to the University of Antwerp are and remain responsible for: the back-up and recovery in the event of loss or theft, the maintenance and management of the ICT system and the data on the system.

6.4 Accounts and passwords

An account is created for each student upon enrolment at the University of Antwerp. With this account, students are granted access to various ICT services of the University of Antwerp such as e-mail, internet, VPN, central network disks for document storage, etc.

Given this extensive access to ICT facilities of the University of Antwerp, each student has the responsibility to protect his or her account with a secure password. The principles that passwords must adhere to are published via Blackboard. In addition, passwords must be changed every six months.

Passwords form the unique access code to the UAntwerp accounts and consequently to the virtual identity of students. It is therefore forbidden to pass passwords on, consciously or unconsciously, to parents, relatives, fellow students or other persons, or to try to find out someone else's password. It is also forbidden to use someone else's account to log in.

Students should change their password immediately if someone else knows it or suspects that someone else has found out.

UAntwerp accounts can only be used to register for activities that are part of the activities of the University of Antwerp. A student may never use the password of his or her UAntwerp account for other personal or professional ICT systems. Examples of other personal or professional ICT-systems are: Facebook, LinkedIn, personal email account, Dropbox, etc.

The above principles apply by analogy to other accounts that provide access to company data or other confidential information or systems related to the University of Antwerp.

7 Communication

7.1 E-mail

It is forbidden to send mass unsolicited and undesired electronic mail (also known as SPAM), viruses, chain letters or hoaxes via or to ICT resources of the University of Antwerp.

If a student wishes to reach all students of the university, he must make a request via the form on Blackboard. The student's message will initially be published on Blackboard.

A student should not send e-mails to large groups of students, unless the subject is education- or study-related in the context of the programme. Examples of what is not allowed are mails about: the sale of second-hand books, classified ads, exam changes, buying or renting a room, etc.

Students should check their mailbox regularly and tidy it up or archive it. The University of Antwerp reserves the right to intervene on the available individual capacity of the mailboxes.

Sending personal e-mails is only allowed as far as this is in accordance with the provision regarding the personal use of ICT resources.

7.2 Internet

For more information on Internet use, please refer to the sections of this standard dealing with personal use and ICT systems.

Regarding the monitoring of students' Internet use, reference is made to the section on supervision and control.

7.3 Telephony

For more information on the use of telephony at the University of Antwerp, please refer to the sections of this standard dealing with personal use and ICT systems.

8 Obligation to report

8.1 Incidents

Breaches of the ICT Code of Conduct, incidents and near-incidents involving ICT resources must always be reported to the ICT Department helpdesk.

An incident can be the physical theft of an ICT resource, but breaking into systems and theft of information are also incidents that must be reported to the ICT department's helpdesk.

The ICT helpdesk can be contacted via the e-mail address helpdesk@uantwerpen.beor by calling 03 265 48 08.

8.2 Incidents with personal data

All incidents involving ICT resources, in which personal data are involved, should be reported to the Data Protection Authority using the data breach notification form without delay.

9 Supervision and control

Within the legal limits, the University of Antwerp can exercise control over data that a student stores, sends or receives within the scope of this standard. Control will take place in a way that limits the interference with personal privacy to a minimum.

Except in the case of incidents, ICT staff may only monitor the use of electronic means of communication in a general manner. For example, a general overview may be drawn up, possibly for each organisational unit, of the websites visited over a certain period and the frequency and volume of information transmitted, but without including any data on individual use.

However, where there is a suspicion that a student is carrying out illegal activities on the network of the University of Antwerp or is in breach of this standard, the University of Antwerp reserves the right to monitor individual activities.

10 Measures in the event of infringement

The University of Antwerp has the right to review and possibly restrict the conditions for the provision of ICT resources when required for business reasons or when legally determined. The University of Antwerp reserves the right to deny access to the network to students who deliberately violate these standards.

The University of Antwerp also has the right to recover costs incurred and/or damage caused from the student.

The University of Antwerp can always take action against violations of this standard by all appropriate means in accordance with the disciplinary measures provided for in the UAntwerp Student Charter.

If illegal activities or information are discovered during checks, the University of Antwerp can report this to the judicial authorities. In case of doubt, further investigation will be carried out in the first instance, during which the individual activities and information can be checked. The University of Antwerp will always cooperate in the detection of crimes and will hand over any user data and log files to the judicial authorities if requested to do so. If it is established that a user has carried out illegal actions in relation to ICT resources, the person concerned will be held personally responsible.

11 Exemptions

Exceptions to this standard can only be granted if there are sound reasons for granting a temporary exception.

Exceptions can only be granted for a limited period of time.

To apply for an exception, the student must submit a reasoned written request to the departmental heads of ICT, Paul Fremau and Geert Vera. If it is decided to grant an exception, this will be communicated in writing to the student concerned.