Guidelines and supervision on the use of IT tools of the University College

Introduction

The employer has the authority to set up guidelines for the use of IT tools that are available for employees and other users. These guidelines are stipulated in section 1 -9.

An IT Deontology Commission supervises the implementation of these guidelines: it will set up a meeting when an update of the guideline is needed or when the implementation is questioned.

The commission consists of the Head of IT, two ombudspersons for staff (one of the former HUB-EHSAL and one of the former KAHO Sint-Lieven), two ombudspersons for students (one of the former HUB-EHSAL and one of the former KAHO Sint-Lieven), one legal expert of the University College and the HR Director.

Supervision on the use of IT tools is stipulated in section 10. Staff with a worker's or employee's status are subject to the Belgian collective agreement (CAO) n° 81 of 26 April 2002 on the protection of privacy of employees with regards to electronic online communication data verification. Due to transparency it is advisable for other staff to abide by this CAO.

The CAO states that verification by the employer on the use of online communication tools is allowed for the employees, on the condition that it is done in a way that it minimalizes the interference in the privacy of the employer.

The organisation of the supervision does not need to be approved by the Works Council in conformity with CAO n° 81. However, first the Council and next the individual staff members need to be informed about it.
In accordance with the Decree of Higher Education this document is submitted (not negotiated upon) to the Negotiation Committee of Higher Education Institutions to the extent that (as stipulated in article 302, §1 of the Decree of Higher Education) article 11 of the Belgian Law of 19 December 1974 on the regulation of relations between the government and the trade unions of its staff is applied.

To create a practicable instrument one text has been developed that states both the guidelines and the supervision and that applies to all users, staff members, students and external parties. The text also elaborates on the principles on use and supervision, as included in the applicable employment regulations.

Possible sanctions in case of violations on the guidelines by staff members are those stipulated in the applicable employment regulations (for appointed/nominated staff members these are called disciplinary measures instead of sanctions). For students a connection with the disciplinary procedure and disciplinary sanctions has been included in the education and examination regulations.

Odisee
Warmoesberg 26, 1000 Brussel
T +32 (0)2-210 12 11
www.odisee.be

This implies that:

- The Director of the Study Area is authorised for the conversation with the student that needs to take place before each decision that can affect the student individually and that the Director of the Study Area can take disciplinary measures with regards to the student (unless the students prefers the disciplinary board to take a decision, in conformity with article 97 of the education and examination regulation).
- The HR Director is authorised for the conversation with the staff member that should take place before each decision that can affect the staff member individually and that the HR Director or General Principal can impose a sanction or disciplinary measure with regards to the staff member.
- The General Administrator or other member of the Committee of Directors is authorised for external users (both for the conversation and for the decision unless that decisions is part of the authority of the Managing Director).

1. Purpose and scope

A lot of IT tools have been made available by the University College for educational, scientific, administrative and communicative purposes. The use of those tools is strongly encouraged to improve the quality of the institution's core activities: education, research and social services. The University College decides which IT tools are supported and which ones are not.

The following rules guarantee a dignified, disciplined and safe use of IT tools.

These guidelines apply to all staff members, external parties with IT facilities of the University College and students registered at the University College, hereafter referred to as 'the user(s)'.

The user is aware that the University College logs the network behaviour of all IT tools and that it can verify the proper functioning of all networks based on those logs. These check-ups are performed within the applicable legal environment.

Staff members who do not have IT tools available for the performance of their professional activities at the University College have the right to consult their professional e-mail address and the intranet of the University College on the work floor on a regular basis. Agreements on this should be reached between the staff members and their immediate superior.

Superiors can set an out-of-office message on the mailbox of a user to ensure continuity of service.

The guidelines apply to all IT tools, IT infrastructure and electronic means of communication and for all data that is sent or saved by systems. The guidelines also apply for IT tools, whether or not property of the University College, which are being used in connection with the University College (e.g. e-mail address of the University College) or in combination with the IT tools of the University College (e.g. access to the Wi-Fi network on the campuses, etc.)

The IT Deontology Commission (hereafter referred to as 'the commission') monitors the implementation of the guidelines[1]. As the IT tools and the legal environment are constantly evolving, the commission will attend regular meetings to assess the guidelines and modify them if needed by changing circumstances. The modified document will be communicated to the users.

[1] The commission consists of the Head of IT, two ombudspersons for staff (one of the former HUB-EHSAL and one of the former KAHO Sint-Lieven), two ombudspersons for students (one of the former HUB-EHSAL and one of the former KAHO Sint-Lieven), one legal expert of the university college and the HR Director.

Any questions, remarks and suggestions about these guidelines can be addressed to the Commission by contacting ICTdeontologie@odisee.be.
In case of urgent matters the Head of IT will be contacted.

2. Deal with information

Each user is responsible for the information that he/she manages and requests in function of his/her own activities.

Access to the applications and data on the computer systems of the University College is only provided to the user who has authorization. The access is individual and cannot be transferred to another user.

All information of the University College with regards to staff, students, research and administrative systems is property of the University College and should be handled with the utmost care.

Some information of the University College is confidential and should be handled with precarious attention. To determine the degree of confidentiality of that information, the risk for the University College of improper disclosure should be assessed, i.e.:

a. Information on the development of new services, research data or more general information, regardless of the form these are saved, of which the University College is a beneficiary.
b. The harm to the image of the University College, e.g. by spreading sensitive information that can lead to negative publicity;
c. A violation of the law, e.g. the law on the protection of intellectual property, in particular the copyrights or the law on the protection of privacy for the treatment of personal data (salary and other payment data, data on staff and student administration, medical personal data, tests/exams, exam results, and others are personal data by this law);
d. Transfer of information of third parties where the University College has concluded a non-disclosure agreement with.

Confidentiality of information is the key principle. Also information that is not explicitly considered confidential cannot be simply disclosed or published. In case of doubt the Commission and/or one of the legal experts of the University College can give advice.

Confidential information cannot be recorded privately unless an agreement has been made e.g. in the case of working at home or use of the cloud. If those agreements change or if they are terminated the information should be returned to the University College or should be destroyed, as the case may be.

Special attention is being paid to portable media that can contain confidential information, such as information saved as a back-up. This media always need to be stored safely. In case of destruction and possible re-use it should be verified that the equipment does no longer contain confidential information.

On the internet (e.g. social media), on personal web pages and blogs it is not allowed to disclose information subject to the University College's copyright or confidential information on other users or the University College unless explicit prior approval.

3. User responsibilities

The user agrees to notify the IT department immediately of malfunctions or abuse of IT tools, IT infrastructure and electronic means of communication or security gaps.

The user who notes that he/she has access to information he/she normally has no authority for, notifies this immediately to the IT department.

The user agrees to use the means of security provided by the University College and to apply the imposed security measures (e.g. change of password).

The user treats all IT infrastructure with the necessary care and caution. Only laptops and mobile peripherals can be moved by the user, unless authorisation is given to move other IT infrastructure.

The user needs to take into account the following rules where they are applicable to the user category:

1. Use of IT tools:
    a. Register and save files in a correct manner on shared locations in order that the users who are functioning as a back-up can have access to the documents;
    b. Keep IT tools in good condition;
    c. Do not leave IT tools unattended and take sufficient safety measures to prevent theft;
    d. Only install or use software on the device for which necessary licences or user agreements are available;
    e. Take sufficient safety measures that discourage violation of the University College's systems and theft of information, for example by:
        a. Close the door of the workplace / shut down the pc in case of absence;
        b. Activate the screen saver of the PC/workstation and other IT tools;
        c. Secure all IT tools that are connected to the network and all confidential and sensitive information that is saved on these IT tools;
        d. Log on from remote locations with secured protocols.

2. Safety of the data that is saved on the systems:
    a. Verify that data does not contain viruses or other harmful software, in particular:
        - Do not turn off the installed virus scanner;
        - Delete a virus, a suspicious e-mail or document immediately; possibly the system or network administrator needs to be contacted first;
        - Check software and data provided by an external network or portable media for viruses and other harmful software (this should be done by the user or by the request of the user);
        - The utmost caution is needed when installing software;
        - Do not install software of illegal or dubious sources;
    b. Read his/her e-mails and archive his/her inbox regularly. If needed, system or network administrators can change the mailbox size, only after prior notification to the user to save the data of his/her inbox in order that it cannot harm the system;
    c. Abide by the existing rules for making a back-up within the organisational unit; if data is put on local hard disks (e.g. laptop, USB stick) the users are responsible for making a necessary back-up;

3. Remain cautious with personal data requests such as the request for an e-mail address;

4. Treat files from unknown sources cautiously, such as attachments;

5. Remain cautious when logging on to the University College network from remote locations;

6. Do not send viruses or virus alerts (hoaxes) from the University College network;

7. Respect general applicable rules of protocol;

Doubts or questions should be addressed to the system or network administrator, the Commission and/or one of the legal experts of the University College.

If needed (e.g. in case of theft or loss) the University College can block all or part of the access to the IT tools that are connected to the University College network. Data and applications on these IT tools can in this case be remotely deleted and devices made unavailable. For external IT tools that are not owned by the University College this is done after consultation with the owner of the IT tool.

If required for organisational, technical or legal reasons the University College can block certain websites, apps, premium rate numbers and (internal and external) access temporarily or permanently.

The owner/user is fully and solely responsible for external IT tools that are not supported by the University College. This responsibility applies both to the implementation of the necessary

security, backup and restore, loss and theft, the maintenance and management of the IT tool and the data saved on the external IT tool.

4. Passwords and logins

Each user is responsible and liable for everything that happens under his/her login and password. All laptops that contain confidential information about the University College should be secured, for example with a start-up password and a screensaver to secure the content of the data as in the best possible way.

Passwords cannot be saved in a visible form (post-it, etc.). Use caution when entering your password (e.g. not when someone is watching).

Users cannot communicate their password to other users or third parties.

Users who can consult files of the accounts, staff, potential employees or students of the University College and users who can consult the electronic online means of communication of staff or students, or who are informed of other confidential data cannot communicate their password to other users or third parties, unless in special circumstances and with express permission of their superior. In this case the password has to be modified as soon as possible.

For social media and networks for personal use the user has to choose a password and login that differs from the login and password of the University College.

5. Personal use of IT tools of the University College

Personal use is subject to the general guidelines for the use of IT tools of the University College.

Only for staff members – users: the University College allows the personal use of its IT tools as long as it has no negative effect on the professional performance of the user. Moreover, personal use must be secondary to professional use. Where applicable the user has to make up for the (professional) performances that have not been delivered.

Where the University College finds excessive personal use of IT tools, it can invoke a disciplinary measure to prohibit the personal use for a definite period of time.

Only for student-users: students always have priority in the use of commonly made available IT tools for study purposes.

For all users: other uses cannot be disturbed by the personal use, the IT infrastructure of the University College cannot be overloaded and no costs can be charged to the University College, otherwise these costs for personal use will be charged to the user.

Users who store and process personal data on IT tools of the University College should be aware that the University College has the authority to access information in exceptional cases that is processed by a user on IT tools of the University College. Superiors can access this information on behalf of staff members if this is absolutely necessary for his/her function at the University College. In this case, the Commission is notified and the user involved is informed (unless this is impossible). The privacy of the user involved is always protected as much as possible.

For the protection of personal data that is stored by the user on IT tools of the University College it is recommended to save these data in a folder on the personal disk[2] with a reference to personal use.
The University College is not responsible for possible loss of personal data that is stored on its IT tools.

6. Unauthorized access

Unauthorized access exists in the following situations:

1. Spread, save or enter information that:
   a. Harm the image, the moral or economic interests of the University College;
   b. Is offensive, defamatory, indecent or discriminating;
   c. Can harm third parties;
   d. Violates the applicable legislation, public order or public morality;
2. Communicate confidential information such as business secrets, personal data etc. to persons who are not entitled to receive this information;
3. Save confidential information in an unsecured way, both electronically and on paper;
4. Copy business data for purposes other than professional or study purposes to locations outside of the University College network without prior written permission. All data should be returned to the University College upon termination of the (cooperation to) task linked to the data.
5. Communicate personally acquired rights of use and licenses of the University College to third parties;
6. Try to obtain passwords and usage data of other users;
7. Create a false identity on the network;
8. Compromise system security or information by
   a. Bypassing internal or external system and network security;

[2] The personal disk is destined for professional use and not for personal use only. It differs from the common disk or collaboration on the intranet in that way that the access to the personal disk is restricted to the individual staff member.

b. Installing or using software without permission or license[3]
c. Violating the legalisation on copyrights and other intellectual rights (e.g. copying software unless this is permitted by the license of the supplier or by law)
d. Connecting IT devices that are not property of the University College without explicit permission of the system or network administrator;
e. Forcing access to non-authorized systems
f. Hacking/eavesdropping the network
g. Informing third parties about security gaps;

9. Distribute a large amount of unwanted or unsolicited (junk) e-mails[4] or chain letters;
10. Disturb other users when performing activities or attempt to disturb a department, network or computer by e.g. overloading a network or a computer;
11. Modify, delete or communicate system information, system configuration, application programs or files to third parties except as authorized;
12. Commercialise internally developed software that forms part of the University College's heritage and that has been developed in the context of the professional or educational activity for personal use or perform acts that can obstruct the further use or exploitation of the software unless it concerns software that is developed to be disseminated without restrictions, e.g. software with an open source code license[5].

If one or several uses as mentioned above are subject of scientific research and as a result a derogation of these guidelines is desired, a request for derogation should be submitted to the Commission by contacting ICTdeontologie@odisee.be.

Each user needs to be aware that the University College is obliged to cooperate with the judicial authorities in the course of enquiries or judicial proceedings.

7. Privacy statement

At least the following users need to sign a privacy statement:

- Users that have access to data from the accounts, staff, potential employers or students of the University College;
- Users that can have access to electronic online communication data of other users such as local system and network administrators;

---

[3] The IT Departments sets out to have 3 separated systems in the future (3 layers): layer 1 is an unsecured network that is accessible for all users (Bring Your Own Device), excluding access back office access (operational environment); layer 2 is a semi-secured system that is accessible to staff members, including back office access; layer 3 is a highly secured system that is accessible for IT staff who are responsible for back up and IT devices. The prohibition in 8.b. only applies for layers 2 and 3.

[4] Spamming

[5] Contractual agreements are concluded with external employees who develop software as part of their function at the University College.

- Users that become aware of personal data in the context of their research activity.

They need to sign this statement upon implementation of these guidelines, or from the moment they have access to or are informed about these data.

8. Access rights for external users

External users who need access rights to IT tools, IT infrastructure or electronic means of communication of the University College to perform their task at the University College (e.g. guest speakers) can only obtain these after signing and dating a statement to the effect that they have received and will comply with the guidelines for IT use at the University College. In this statement they will indicate their full name, address and phone number.

The access rights are allocated in a personal capacity and only apply for the period that is needed to perform the task.

9. Termination of employment (only for staff members)

The staff member who is leaving the University College abides by the rules of the document "IT use in case of and after termination of employment". This document can be consulted on the intranet or can be obtained from the HR Department.

10. Supervision on the use of IT tools

Checks are carried out by staff members who are in charge of the system and network management or parts of these, especially the system and network administrators, in a way that limits interference with privacy. Individual checks can be carried out in response to incidents or a cooperation request of the judicial authorities.

For staff users

CAO n° 81 of 26 April 2002 on the protection of the privacy of employees applies to staff members with a worker's or employee's status as the supervision of electronic online communication data is concerned (hereafter referred to as the "CAO")[6]. This CAO applies also to other staff members.

[6] The CAO applies to the supervision of electronic online communication data in the broad sense, irrespective of whether this concerns internal or external online communication. This also includes the e-mail traffic between employees during working hours. CAO n° 8 explicitly states that it does not wishes to regulate some elements, in particular regulations for the access to and/or use of electronic online means of communication of the University College: this remains the prerogative of the employer.

The CAO states that supervision by the employer on the use of online means of communication is allowed by the employees. It should, however, be carried out in a way that limits interference with privacy.

Staff members are collectively (through the HOC) or individually (through the intranet) informed on the implementation of a possible general check-up. Individual checks can be carried out in response to an incident or a cooperation request by the judicial authorities.

Checks are carried out in the light of the CAO objectives, in accordance with the applicable labour regulations:
1. Prevention of unauthorized facts;
2. Protection of (confidential) interests of the University College;
3. Security and proper functioning of IT network systems;
4. Compliance (in good faith) with the guidelines for IT use at the University College.

If it only concerns the non-compliance of objective 4, individual checks can only be carried out after a reminder of the guidelines.

An incident is investigated:
- After establishment of a technical incident by the IT Department;
- After an incident is internally reported by another user;
- After an incident is externally reported by contracting parties of the University College (e.g. company for the traineeship);
- After an official cooperation request by the judicial authorities.

If the investigation shows that one of the objectives has been violated, the HR Director is informed of the result of the investigation. The HR Director will then discuss this with the staff member before a decision is made that can harm the staff member. The staff member will have the opportunity to raise objections with regards to this decision. He/she can also opt to be assisted by an union representative. Disciplinary measures can be taken (e.g. temporary prohibition of personal use) and/or a sanction or disciplinary measure that is included in the labour regulations. Criminal offences are reported to the competent authorities.
If needed protective measures can be taken to ensure the security and integrity of the IT systems and related processed information.

For student users

An incident is investigated:
- After establishment of a technical incident by the IT Department;
- After an incident is internally reported by another user;
- After an incident is externally reported by contracting parties of the University College (e.g. company for the traineeship);

- After an official cooperation request by the judicial authorities.

If the investigation shows that the IT guideline or legislation has been violated, the Director of the Study Area is informed of the result of the investigation. The Director of the Study Area will then discuss this with the student before a decision is made that can harm the student. The student will have the opportunity to raise objections with regards to this decision. A disciplinary procedure may be initiated in accordance with the education and exam regulations. Criminal offences are reported to the competent authorities.
If needed protective measures can be taken to ensure the security and integrity of the IT systems and related processed information.

For users other than students and staff members

An incident is investigated:
- After establishment of a technical incident by the IT Department;
- After an incident is internally reported by another user;
- After an incident is externally reported by contracting parties of the University College (e.g. company for the traineeship);
- After an official cooperation request by the judicial authorities.

If the investigation shows that the IT guideline of legislation has been violated, the general administrator is informed of the result of the investigation. The general administrator or another member of the Executive Committee will discuss this with the user before a decision is made that can harm the user. The user will have the opportunity to raise any objections with regards to this decision. Criminal offences are reported to the competent authorities.
If needed protective measures can be taken to ensure the security and integrity of the IT systems and related processed information.