Using ICT resources at KU Leuven
Code of Conduct for Students

1. Purpose and scope

1.1. ICT: an integral part of the educational experience

KU Leuven makes a vast array of ICT resources and ICT-related services available to its students for educational, academic, administrative and communication purposes. The use of these resources is strongly encouraged in order to improve the quality of the university’s core activities: education, research and service to society. ICT is an integral part of the educational experience, and actually plays a key role in it.

All students who are enrolled at KU Leuven are entitled to participate in education and training. When the use of ICT resources is either requested or required for these purposes, each student, in accordance with his or her specific enrolment status, must be able to utilise the centrally- or decentrally-provided ICT resources and ICT services. The Academic Authorities determine which rights and obligations are to be associated with this enrolment status.

1.2. Purpose of this document: codification of agreements

KU Leuven has legal and moral obligations to implement security measures for ICT resources and the information handled by these ICT resources in order to protect individual students, KU Leuven and its partners. In addition, a number of agreements are necessary in order to prevent abuses and to guarantee the efficient and proper use of, among other things, the network and systems. Among other things, this Code of Conduct contains a summary of the current laws governing the use of ICT resources specifically as they relate to students at KU Leuven.

---

1. see appendix: overview of centrally provided ICT resources and services
2. KU Leuven also maintains a Code of Conduct for staff that is analogous to this Code of Conduct for students: https://admin.kuleuven.be/intranet/beleidsinformatie/200514.html.
The goal of this document is to codify both rights and obligations into a Code of Conduct and to specify the procedures to be taken in the event that it is violated.

For the sake of clarity, this ICT Code of Conduct contains several lists of examples. These lists have only been included for purposes of illustration, however, and due to continuing advances in technology they should never be considered exhaustive.

1.3. Scope

The Code of Conduct for students set out below applies to all ICT resources, IT infrastructure, electronic communications devices (including telephones, Unified Communications applications (among others, IP telephony, video conferencing, IRC, etc.), mobile phones, PDAs, tablets, faxes, PCs, laptops, pagers, modems, e-mail, messaging/chat, blogs, forums, internal memo systems, network software, internal and external networks, internet, LAN, learning and testing platforms, administrative systems, information systems, etc.) and to all data transmitted by or stored in these systems, as well as the ICT services provided by KU Leuven to its students. This Code of Conduct also applies to the use of ICT resources - whether or not they are the property of KU Leuven - which are used in association with KU Leuven (such as a KU Leuven e-mail address) or in combination with the ICT resources of KU Leuven (such as access to KULeuvenNet, KotNet, etc.).

This Code of Conduct applies to all students at KU Leuven.

The ICT Code of Conduct Committee3 (e-mail address: netdeon@kuleuven.be) monitors the strict adherence to the deontological rules set out below.

2. Rules governing utilisation

KU Leuven expends a great deal of effort to provide ICT services and resources for the best possible price and to set and maintain the entry threshold for all students as low as possible. The “proper use” of the services and resources provided is essential to the continued development of these efforts.

The rules set out in this Code of Conduct are intended to guarantee the respectful and disciplined use of ICT resources.

The utilisation rules below serve as basic set of rules in this respect, and they are intended to be applied in combination with specific or more targeted rules which apply to specific systems or applications. As such, specific centrally or decentrally drafted regulations governing the use of these ICT resources and ICT services must conform to this Code of Conduct.

Students must constantly be aware of the fact that KU Leuven logs the network behaviour of all ICT resources and that KU Leuven is always able to monitor the proper functioning of its networks on the basis of these logs. This monitoring is always conducted within the current legal framework.

If a student believes that one or more of the uses which are defined as unauthorised in the list below constitute an integral part of the educational experience and/or of academic research, then he/she must submit a well-founded request for an exception to his/her lecturer. This lecturer will then in turn submit a request to the ICT Code of Conduct Committee (e-mail address: netdeon@kuleuven.be) to have certain aspects of that specific case exempted from this Code of Conduct. The request will be analysed by the Network Deontology Committee and based on this analysis a temporary exception may be allowed. Once an exception is allowed, it must be re-evaluated at regular intervals.

2.1. Authorised use

Students are allowed to make use of the ICT infrastructure of KU Leuven to exchange information, express their opinions, etc. as long as this complies with the law and is consistent with a basic sense of etiquette, respect and courtesy. Each student has a responsibility in this regard towards his/her fellow students, the university as a whole, and society.

KU Leuven allows students to utilise the available ICT resources to the extent that this use conforms to this Code of Conduct and to applicable laws.

---

3 See appendix: Composition and functions
For its part, KU Leuven is committed to ensuring that a number of basic services and needs are met, such as providing an e-mail address and offering PC classes with internet access. When third parties are involved (such as KotNet: ISP Providers), there are a number of ICT services which KU Leuven is not always able to guarantee.

2.2. Unauthorised use

The communication resources made available by KU Leuven may under no circumstances be used for the processing or transmission of unauthorised information.

Unauthorised information can be seen as, among others, the elements listed up below.

KU Leuven does not permit the use of ICT resources (this list is not exhaustive):

1. for the distribution or storage of information that:
   a. might harm the image or the moral or economic interests of KU Leuven. This in no way compromises one’s right to criticise policy;
   b. is insulting, defamatory, offensive or discriminatory (such as pornographic material or information that is contrary to the generally applicable rules of decency);
   c. could inflict harm on third parties;
   d. is incompatible with public order and common decency;
2. to pass information which is characterised as confidential or which, due to its nature, must reasonably be considered confidential (e.g., the intranet, non-published research results, trade secrets, personal information, information concerning colleagues and students, geolocation data, etc.) to persons who are not entitled to receive, distribute or publish this information;
3. to leave confidential information in an unprotected state in either electronic or hardcopy form;
4. to copy university data, either fully or partially, and store it in locations outside the network of KU Leuven for purposes other than those related to work or study without the prior written consent of KU Leuven; for work-related or study-related uses, all data must be returned to KU Leuven at the conclusion of the assignment or once the employee or student has completed work on the assignment with which the data is associated;
5. to pass on user privileges and licences that have been personally acquired from KU Leuven to third parties;
6. to commit unlawful acts by means of:
   a. distributing or storing information which does not comply with applicable laws (e.g., the law on privacy protection in relation to the processing of personal data, copyright law or laws governing electronic communications);
   b. installing or using software for which the competent authority has not granted its consent or which has not been properly licenced;
   c. infringing upon copyright law or other intellectual property rights (such as by making a copy of software in cases when this is not otherwise permitted by the vendor’s licence or the law);
   d. assuming a false identity on the network;
7. to distribute, outside the bounds of normal communication within KU Leuven, unwanted or unsolicited bulk electronic mail (spamming, phishing, etc.) or chain letters (including hoaxes, etc.);
8. to acquire the user data and passwords of third parties via unauthorised means (including phishing, sniffing, etc.);
9. to engage in actions which could compromise the security of systems or information, such as, for example:
   a. bypassing internal and external system and network security (the security of a computer, network, user ID, etc.) in such a way as to penetrate these systems for purposes of undermining operational security or causing harm;
   b. developing harmful software (such as Trojan horses, viruses, worms, etc.) on the systems of KU Leuven or knowingly installing and/or inducing other users to use such software;
   c. knowingly and forcibly gaining inappropriate and unauthorised access to systems which one is not authorised to access;
   d. eavesdropping on the network;
10. to knowingly interrupt other users from engaging in their activities or to make attempts to disrupt any service, network or computer (such as by overloading a network or computer or by attempting to crash a system, etc.);
11. to modify, to remove or to pass on to third parties system information, system configuration information, application programmes or files, unless otherwise authorised to do so by virtue of one’s position;
12. to connect ICT equipment that is not the property of KU Leuven and that does not comply with the security rules specified in this document without the written or implicit consent of the system or network administrator;

13. to profit personally by commercial means from internally developed software that forms a part of the patrimony of KU Leuven and which was developed within the scope of a professional or educational activity, or to carry out acts which could impede the continued use or development of the software, unless it involves software that was specifically developed to be distributed freely (such as software with an open-source licence); contractual agreements must always be negotiated with external collaborators who develop software within the scope of their duties at KU Leuven;

14. for personal uses other than those which are permitted under section 2.4 of this Code of Conduct.

When in doubt, further information and assistance can be obtained by contacting the ICTS Technical Unit at: ICTincident@kuleuven.be.

2.3. Responsibilities of the student

The student has a number of responsibilities which, to the extent they apply, encompass:

1. the use of the ICT resources:
   a. keeping the ICT resources provided in good condition;
   b. ensuring that ICT resources that have been personally provided are not left unattended (such as a rented PC) and taking adequate safety precautions in order to minimise the risk of theft as much as possible; in the event of theft, the ICTS Service Desk (https://admin.kuleuven.be/icts/english/servicedesk) or the ICTS PC Lab (https://admin.kuleuven.be/icts/services/pclab/) must be contacted as soon as possible and the student must also change his/her KU Leuven password as soon as possible;
   c. taking adequate safety precautions to minimise as much as possible the likelihood of KU Leuven systems being infiltrated and (confidential) information being stolen, including (this list is not exhaustive):
      1. never sharing a username and password with third parties (e.g., colleagues, ICTS Service Desk, helpdesks in general, students/student employees, trainees, consultants, external staff, via e-mail, on unknown websites or locations, etc.), this in view of the fact that each user is responsible and liable for all activity associated with his/her login and password;
      2. locking the study area or residence when leaving for periods other than a very brief and incidental absence;
      3. enabling the screensaver on the PC/workstation and on other ICT resources;
      4. logging out when finishing work on a workstation in the PC classes;
      5. securing all ICT resources connected to the network (among others, laptops, mobile phones, smartphones, tablets, USB sticks, etc.) and all confidential and business-sensitive information that is stored on these ICT resources (by making use of a power-on password, PIN code, screensaver, firewall, data encryption, etc.);

2. the security of the data stored in the systems:
   a. verifying that the information that has been received is free of any virus that could compromise the proper functioning of KULeuvenNet and KotNet:
      1. it is forbidden to disable the virus scanner installed on the systems of KU Leuven, except in very exceptional circumstances and only with the express consent of the system administrator;
      2. it is forbidden to use a (personal) computer that does not have a virus scanner installed or to disable this software, with exception for cases in which this is explicitly allowed. It is moreover essential that this software be updated on a regular basis.
      The campus licences enable each student to download a free anti-virus programme for personal use: https://admin.kuleuven.be/icts/services/software;
   3. software and data which have been acquired via an external network, via web applications (e.g., webmail, webhosting, etc.), via external ICT resources (e.g., smartphones, tablets, laptops, etc.) or via portable media (such as diskettes, ZIP disks, CD-ROMs, DVDs, USB sticks, etc.) must be checked for viruses and other malicious software;
   4. when confronted with a virus, a suspicious e-mail, a suspicious document or a document of unknown origin, work must be stopped immediately and the
suspicious e-mail or suspicious document removed; if necessary, the local system or network administrator or the ICTS Service Desk must be contacted;
5. the highest degree of caution must always be taken when installing software or using data that has been acquired via an internal or external network;
6. it is never permitted to install software of dubious origin;

b. reporting incidents, any shortcomings in the security of the computer system, or methods which could compromise the security of data, to the network and system administrators (e.g., the network administrator of a residence hall) or to the ICTS Service Desk. Third parties may not be made privy to this information. Any exploitation of these weaknesses shall be viewed as (an attempt at) infiltration;
c. reporting violations of the Code of Conduct to the ICTS Technical Unit at ICTincident@kuleuven.be;

3. accessing his/her student e-mail account and reading his/her e-mails at regular intervals, as well as emptying out the mailbox and archiving old e-mails if necessary. All official electronic communications from KU Leuven to the student are sent to this e-mail address. E-mail can be lost if the mailbox exceeds its maximum capacity. System administrators are moreover permitted to take steps to free up space in a mailbox by deleting e-mails once the available capacity of the mailbox has been exceeded;
4. taking precautions when handing out personal information such as one’s e-mail address, mobile phone numbers, addresses, etc. This can be a source of potential abuses, such as spam;
5. taking precautions with files (e.g., attachments) of unknown origin and never opening them if one is not certain of either the contents or the recipient;
6. taking precautions when logging into the KU Leuven network from other, external (public) locations (e.g., when logging in via cybercafés or open/public wireless networks, etc.);
7. not sending viruses or virus notifications (hoaxes) from the KU Leuven network;
8. observing the rules of internet etiquette, or netiquette (link: http://web.inter.nl.net/users/Maurice.Makaay/).

When there are doubts or questions concerning the above points (as to whether something is of “dubious origin” or regarding suspicious e-mails or documents, etc.), the system or network administrator or the ICTS Service Desk must always be contacted.

KU Leuven determines which ICT resources are supported and which are not.

When necessary (e.g., in the case of theft, loss, etc.), KU Leuven may fully or partially block access by ICT resources (such as smartphones, tablets, laptops, etc.) that are connected to the KU Leuven network. In the case of administered devices or devices that are registered with KU Leuven, KU Leuven may remotely erase the data and applications on the ICT resources and, if necessary, render the devices unusable. In the case of external ICT resources which are not the property of KU Leuven, this will be carried out in consultation with the owner of the ICT resource.

Students take full, individual responsibility when installing illegally downloaded material (e.g., software, files, music files, video files, etc.) via the ICT resources of KU Leuven. KU Leuven always cooperates fully with legal investigations into such activities;

**Personally-owned, external ICT resources**

Personally-owned ICT resources that are connected to the KU Leuven network must also comply with the rules laid down in this Code of Conduct. For ICT resources which are unsupported, it is the responsibility of the owner/user to ensure that all essential security features have been deployed on the external ICT resource.

KU Leuven can never be held responsible when problems arise with external ICT resources (e.g., personally-owned tablets, smartphones, laptops, etc.) which are neither administered nor supported by KU Leuven. It is the responsibility of the owner of the external ICT resource to back up the data stored on the external ICT resource. The owner of personally-owned ICT resources bears the risk associated with these resources. As a result, the user who connects his/her own external ICT resource to the KU Leuven network is and remains responsible for its back-up and restore, its loss or theft, the maintenance and management of the ICT resource, as well as the data stored on that resource.

---

4 A list of all the network administrators can be found at: http://cwisdb.kuleuven.be/persdb-bin/netadmin
2.4. Authorised personal use of KU Leuven ICT resources

KU Leuven allows the personal use of KU Leuven ICT resources within reasonable bounds.

Within the reasonable bounds in which the personal use of ICT resources is permitted, the following applies:

a. this use must not interfere with the studies or research activities of others;

b. barring other agreements, KU Leuven is not responsible for the costs associated with this use;

c. priority is given to study purposes when making use of the shared ICT resources made available.

KU Leuven allows the personal use of KU Leuven ICT resources in PC classes and via KotNet with the understanding that the University, when required for organisational or technical reasons or when it is legally obliged, expressly reserves the right to:

a. revise the terms and conditions that apply to the ICT resources provided and, if necessary, restrict or suspend them;

b. recover any additional costs from the user which have been incurred further to his/her personal use;

c. at any time and without prior warning, block and (temporarily or permanently) prohibit access to certain websites, apps, premium-rate numbers and (internal and external) access channels.

All statements in this ICT Code of Conduct apply also for personal use.

Users who store and process personal information on the ICT resources of KU Leuven must be aware of the fact that KU Leuven may, in exceptional cases, obtain access to information that is processed on its ICT resources.

If KU Leuven determines that it is necessary to access this information, a request must always be submitted to the ICT Code of Conduct Committee (e-mail address: netdeon@kuleuven.be). In such a case, the person in charge of Student Affairs will be notified. KU Leuven shall always inform the student in question that specific information belonging to this user is being accessed, unless this is impossible for a particular reason (i.e. death, as part of specific legal investigations, etc.). Every effort shall be made in each case to protect the privacy of the user in question to the greatest extent possible.

Personal webpages are permitted as long as they do not exceed the disk space that has been allocated for them on the servers of KU Leuven (https://admin.kuleuven.be/icts/services/webspace). This disk space includes space that has been allocated for both e-mails as well as the storage of other files (e.g., HTML pages).

The following applies here:

a. this information must conform to the rules specified in sections 2.1, 2.2 and 2.4;

b. the information that is made available via these webpages must include a disclaimer, which can be found at: http://www.kuleuven.be/cwis/disclaim_en.htm;

c. the name of the author must be clearly noted on each page;

d. the author bears full responsibility for the content of the webpages;

e. the style of personal webpages must be clearly distinguishable from the digital house style used by the Communications Department: http://www.kuleuven.be/communicatie/;

f. the use of these services can be restricted by KU Leuven if such use overloads the systems or overly interferes with routine activities;

g. KU Leuven reserves the right to take webpages offline if they are not consistent with the Code of Conduct.

2.5. Passwords and usernames

Access to the computer infrastructure and the network is granted via individual user authentication.

Once someone is connected to a network or computer system, he/she must abide by the rules governing the handling of information (see section 3). For centralised applications, there are guidelines for managing and using global KU Leuven passwords:


A username must be secured by means of a well-chosen password. The following rules, among others, apply to passwords:
a. a password must be changed on a regular basis, and must be changed immediately upon the request of the system or network administrator (such as when an incursion has been detected or when the password is too weak);

b. for all applications, choose a complex password that complies with the KU Leuven password policy;

c. if there is even the slightest suspicion of improper use of the username and password, the password must be changed as soon as possible;

d. no one is permitted to give out his/her password to third parties (such as fellow students, trainees, helpdesks such as the ICTS Service Desk, student employees, external staff, via e-mail, on unknown websites or locations, etc.) and/or allow third parties to use it;

e. no one is permitted to use someone else’s username;

f. it is forbidden to try to hack or otherwise obtain the passwords of others;

g. it is not permitted to store or to use passwords in a visible form (such as on Post-it notes, in unprotected files, etc.);

h. caution must be used when entering passwords (e.g., doing so only when no one is looking, etc.);

i. caution must be used when entering passwords in unsupervised locations or networks (in cybercafés, in other (open/public) wireless networks, etc.);

j. the KU Leuven username and password must only be used to gain access to the KU Leuven network and KU Leuven applications. Usernames and passwords used on the internet and for personal ICT resources must be different from the username and password used to gain access to the KU Leuven network.

Each user is responsible and liable for all activity associated with the use of his/her user ID and password.

It is recommended that, where possible, all ICT resources (e.g., smartphones, laptops, tablets, mobile phones, etc.) be secured by means of a power-on password or PIN code, as well as a screensaver, in order to protect the integrity of the data as much as possible.

3. Handling of information

The Code of Conduct applies to all information irrespective of the way in which this information is:

a. communicated (via hardcopy, in electronic form, verbally, etc.);

b. stored (in text form, in administrative systems, databases, on websites, in testing and learning platforms, etc.);

c. distributed (via e-mail, directory, website, fax, telephone, etc.).

The Code of Conduct presumes that each student is responsible for the information that he/she manages and for the information that he/she requests within the scope of his/her studies. The use of information is restricted to that required in order to carry out the educational and training assignment, including all study-related activities, participation, co-management, specific issues related to student employment, etc.

With the exception of other rules which have been explicitly stated, the authorisations which grant access to the applications and data on the computer systems of KU Leuven are personal and non-transferable.

All information of KU Leuven related to staff, students, research and administrative systems is the property of KU Leuven and must be handled with utmost care.

Certain information of KU Leuven is confidential, and special care must be taken when handling this information.

In order to determine the level of confidentiality for a piece of information, one must consider what the potential risk would be in general if this information were to be improperly distributed, as well as what the more specific implications would be for KU Leuven, such as:

a. the loss of economic value (e.g., information concerning the development of new products and services, research data or more general information to which the University is entitled, irrespective of the form in which it is stored);

b. harm to its reputation (such as the dissemination of sensitive and confidential information resulting in negative publicity);

c. a violation of the law and internal regulations (e.g., the law on the protection of intellectual property rights and especially copyrights (distributing texts or images belonging to third parties without permission, etc.), the law on privacy protection in relation to the processing of personal data (salary and other payment data, information concerning staff and student administration, personal medical information, test/exam papers, exam results and other personal information covered by...
this law), the transfer of information originating from third parties that is subject to a non-distribution agreement, the illegal downloading or copying of software or files, etc.;

d. a violation of the internal regulations of KU Leuven (e.g., the rules governing intellectual property rights to research results
e. a violation of a non-distribution agreement (e.g., the transfer of information originating from third parties subject to a non-distribution agreement that carries the risk of major compensation resulting from a breach of contract).

When in doubt, information must be considered confidential, regardless of whether or not that information has been branded with a confidentiality label. Advice can be sought from the owner of the information or from Student Legal Services.

 Regardless of how confidential the information in question may be, a specific access level must also be assigned to this information. It is not by definition permissible to publicly distribute a piece of information just because it has been labelled non-confidential.
This is why it is advisable not to leave documents behind on printers or in classrooms.

In principle, confidential information may not be stored outside KU Leuven (e.g., on a personal PC, on ICT resources which are not the property of KU Leuven, in cloud storage, etc.).
While it is permitted to do this in the context of study-related activities, it is only permitted for the time during which this is strictly necessary and in situations in which this is required.
Once both of these conditions cease to apply, this information - depending on the specific situation - must be returned, removed or destroyed.

Special care must be taken when using portable media (for making back-ups, etc. and for hardcopy documents) which contain confidential information. Such media must always be stored in a safe place.
When destroying or possibly recycling ICT resources, one must be certain that these ICT resources no longer contain any confidential information. When destroying confidential documents, one must moreover be certain without a doubt that such destruction is guaranteed.

Finally, it should be pointed out that, unless special measures are taken, any information that is transmitted via the network can theoretically be read, modified or recovered. As such, users must be aware that the protocols most commonly used on the intranet/internet contain no built-in functionality to guarantee the confidentiality of communication. There are several ways in which information can be read, modified or tampered with in the course of being transmitted. Users who would like to distribute confidential information securely - via electronic mail for instance - must take additional measures (including data encryption, secure protocols, etc.).

4. Supervision and monitoring

A. Fundamental right to monitor

Within the limits of the law, KU Leuven is entitled to monitor the data that are stored, transmitted or received by a user within the scope of this Code of Conduct. Monitoring shall occur in such a way as to minimise the degree to which the privacy of students is intruded upon.

Monitoring shall be carried out by persons who are responsible for administering systems, networks or components thereof (system and network administrators) as part of their professional functions. In the course of their everyday responsibilities, these persons are in a position to supervise the use of (a part of) the computer systems and the networks of KU Leuven. By virtue of this authority, they are bound by a stringent set of conditions with respect to the protection of user privacy and always exercise discretion when performing operations.

System and network administrators are permitted to conduct any type of monitoring that constitutes an inherent part of the administration of information systems and networks in order to guarantee the proper functioning thereof and in order to prevent or remedy overloading or security issues. All students must be aware of the fact that this potential for monitoring exists and that any communication they exchange via the network may be subject to this monitoring.
Except in the case of incidents, or under the conditions which are described below (under "Incident handling procedure"), system and network administrators are only permitted to monitor the system-wide use of electronic communication devices in a general manner.

B. Incident handling procedure

An incident is an action or a circumstance which interferes with the normal operation of the computer system or the network. For purposes of implementing this Code of Conduct, a distinction is made between two different types of incidents:

- technical incidents
- violations of the rules of conduct

B1: Procedure in the event of technical incidents

In the course of performing their administrative duties, system and network administrators must frequently contend with technical incidents. For example, users of the systems or networks for which they are responsible can become the victim of computer viruses or other undesirable phenomena (network overloads, etc.). System and network administrators are allowed to act independently to resolve these incidents when a given incident involves only the system or network for which they are personally responsible and does not affect anything outside its bounds. In the course of resolving this incident, they are permitted to immediately identify the students and monitor their network activity at the individual level as long as this is necessary to resolve the incident and as long as monitoring is needed to prevent a recurrence of the problem. Students are notified of this in these instances, and the system and network administrators may contact the student in question if this is necessary to remedy the problem.

In cases where it is necessary to ensure the security and proper functioning of the network, the system and network administrators may (on a temporary basis) immediately and without prior notification block (sub)networks or other access channels (e.g., e-mail addresses, directories, firewall settings, etc.) or take other (temporary) measures in order to prevent a situation from deteriorating and to guarantee the security and integrity of the University’s ICT systems and information. When necessary, a student must, at the request of the system and network administrators, immediately disconnect from the KU Leuven network the internal ICT resources and the external ICT resources that are not the property of KU Leuven.

B2: Procedure in the event of violations of the Code of Conduct

In the event of violations of the rules contained in the Code of Conduct, one or more of the following procedural steps shall apply, depending on the severity of the violation.

Reports and their handling

Anyone who determines that the rules of this Code of Conduct have been violated must report this to the ICTS Technical Unit at ICTincident@kuleuven.be. Persons who are allowed to report incidents include users, students, supervisors, system and network administrators, or third parties. If someone has a reason that prevents him/her from notifying the ICTS Technical Unit of the violation, he/she has the option of reporting this violation via the ombuds services5, who can then pursue the complaint further.

The ICTS Technical Unit observes the following procedure:

1. When it appears that none of the rules of the Code of Conduct have been violated: the ICTS Technical Unit will handle the report itself on an informal basis and will provide the person submitting the report with a clear explanation as to the reasons why no further steps are necessary; if the person submitting the report does not accept the explanation offered by the ICTS Technical Unit, the subsequent procedural step will be followed.

2. When one or more of the rules of the Code of Conduct appear to have been (seriously) violated: the ICTS Technical Unit will investigate the violation that has been reported in order to determine the actual facts of the case, with the assistance of the local system or network administrator when required. In the course of this investigation, a file will be created to document these facts.

5 http://www.kuleuven.be/education/regulations/index.php#afd62
If deemed necessary by the ICTS Technical Unit or the relevant system and network administrators, temporary precautionary measures may be taken immediately by the system and network administrators in order to prevent further irregularities from occurring. In the event that the unauthorised use constitutes a crime or presents a serious threat to the financial or economic interests of KU Leuven, the student in question may - without further notification - be subject to further monitoring for purposes of gathering evidence. In such a case, the Vice Rector for Student Affairs will be immediately notified of the circumstances.

The ICTS Technical Unit always provides the Vice Rector for Student Affairs with the file. Depending on the severity of the violations and the damage inflicted upon KU Leuven, the Vice Rector of Student Affairs may initiate a disciplinary procedure, which may be accompanied by penalties through the application of the regulations on education and examinations (http://www.kuleuven.be/education/regulations/index.php#afd63).

**Miscellaneous**

a. Legal inquiries

All persons subject to this Code of Conduct must be aware of the fact that KU Leuven will cooperate fully with legal inquiries and will inform the legal authorities if the circumstances require such action.

b. External Communications

When necessary and when applicable, external communications regarding ICT incidents at KU Leuven, particularly via the media or the internet, must be made solely by the Communications Department in consultation with the Vice Rector for Student Affairs.

5. **Follow-up**

The guidelines contained in this Code of Conduct are related to ICT resources that are constantly changing. For this reason, this Code of Conduct may be modified or supplemented, on a yearly basis or any time that the situation requires it, by the ICTS Technical Unit by means of minor changes (new ICT resources, updated links, etc.), minor additions (supplemental examples, etc.) or clarifications. The ICT Code of Conduct Committee will be notified every time that changes are made to the Code of Conduct.

Every two years or in the event of major changes (e.g., additional clauses, additional rules, changing options for monitoring, etc.), the ICT Code of Conduct Committee will convene to check to see whether the Code of Conduct and the security policy are compatible with the new circumstances and with existing laws, and to make any adjustments that are necessary. The new proposal will be resubmitted for ratification to the Council for Student Facilities and the Academic Council.

All questions, comments and suggestions related to this Code of Conduct can be directed to the ICTS Technical Unit via e-mail at ICTgedragslijn@kuleuven.be.

KU Leuven reserves the right to amend this policy at any time. All authorised users will be notified of any changes made.

The Code of Conduct was approved by the Executive Board on 18/06/2013 and approved by the Academic Council on 25/06/2013. It will come into force at the start of the 2013/2014 academic year, to remain in effect indefinitely.
Appendix: overview of centrally provided ICT resources and services

The following ICT services and ICT resources are “centrally” provided to students of KU Leuven (to whom they apply) via ICTS\(^6\) (https://admin.kuleuven.be/icts/english/students - this list is not exhaustive and includes only the most significant services and resources):

All enrolled students receive an intranet user ID and password when registering. This intranet user ID will remain the same for the remainder of the student’s academic career at KU Leuven. This intranet user ID and password will allow a student to login to the Central KU Leuven Login. A range of (centralised) applications, such as the university e-mail account, KU Loket or the electronic learning environment, require the use of this central login.

All enrolled students are also allocated web space for e-mail with an address that takes the form of firstname.lastname@student.kuleuven.be as well as a limited amount of space on a webserver of KU Leuven for storing personal webpages, etc. E-mail is an important communication channel to and from KU Leuven.

A centralised back-up is made of this personal mailbox and these personal webpages. The centralised back-up is designed to allow files to be restored in the event of a system failure. It is not possible to restore individual mailboxes or webpages from this centralised back-up, so it recommended that critical files and directories also be backed up to portable media (burned to CD-ROM, DVD, USB stick, external hard drive, etc.) at regular intervals. KU Leuven cannot be held liable for any loss of data.

The centrally-supported virtual electronic learning environment, which is provisioned by Toledo (http://toledo.kuleuven.be/english), is intended to encourage students to participate in educational and research activities. This dovetails with KU Leuven’s core educational concept of “Guided Self-Study”: http://www.kuleuven.be/studenten/eerstejaars/zelfstudie.html.

Via the Central KU Leuven Login, any student to whom it applies can login to the KU Loket in order to access the following applications: the student’s file, the student’s personalised schedule, the student’s progress file, the individual course programme (http://www.kuleuven.be/onderwijs/is/), the individual exam schedule (IER), etc.

KotNet (https://admin.kuleuven.be/icts/services/kotnet) is designed to make it as easy as possible for students to connect to KULeuvenNet (http://kulnet.kuleuven.be/) and to the worldwide internet from home or from their campus residence, and in so doing to expand their study and research options. The transmission of data to and from the worldwide internet takes place mainly over this network, which has been built up by KU Leuven over the years.

Wireless access is generally available to both the internet and the intranet within the buildings of KU Leuven. This wireless network is called Eduroam (https://admin.kuleuven.be/icts/english/wifi).

The PC classes (https://admin.kuleuven.be/icts/english/pcrooms/index) are intended to lower the access threshold for the use of computers and computer software as much as possible. The computers which are used in the computer classes also provide access to the worldwide internet.

The PC Rental Service (https://admin.kuleuven.be/icts/services/pcshop/verhuur/) makes desktops and portable PCs available to students at a reasonable price. This equipment remains the property of KU Leuven throughout the rental period.

The most popular hardware and software products can be purchased at the PC Shop (https://admin.kuleuven.be/icts/services/pcshop/index.html/) at advantageous prices. A distinction is made between in-store sales (stock items such as PC supplies, hardware peripherals, etc.) and transit sales (special-order items such as desktops, printers, notebooks, software, accessories, etc.).

\(^6\) ICTS – Information and Communication: Technology and Systems: ICTS is the main ICT department at KU Leuven. ICTS is responsible for providing centralised ICT support for education, research, administration and policy. ICTS manages the centralised IT infrastructure, the central databases, all servers (mail server, webserver, etc.) as well as the High Performance Cluster for scientific computing. More information on ICTS can be found at https://admin.kuleuven.be/icts/english/.
The PC Lab (https://admin.kuleuven.be/icts/services/pclab) provides support for hardware and software problems. In addition to advice it also provides practical support during set-up, installation and the detection of problems in close cooperation with the ICTS Service Desk (https://admin.kuleuven.be/icts/english/servicedesk).

The ICTS Service Desk (https://admin.kuleuven.be/icts/english/servicedesk) is the direct link between all computer users of KU Leuven and ICTS. It serves as a clear point of contact for anyone within KU Leuven who needs reliable computer and/or communications support but who maintains no direct contact with ICTS. This ICTS Service Desk provides first-tier support for a range of computer problems. This helpdesk is reachable via e-mail at all times and via telephone during business days.

Students can take advantage of the Campus Licences (https://admin.kuleuven.be/icts/services/software) that have been made available for the use of software. The terms and conditions of their use are listed on each software product.

Students may also, at no obligation whatsoever, take a number of courses or training sessions (https://admin.kuleuven.be/icts/english/trainings/eng_training) on the most commonly-used office applications, operating systems and scientific software. The curriculum is regularly adjusted to meet existing needs, and the courses are repeated at regular intervals. Access to these courses is provided for a low price.

**Appendix: Composition and functions**

**ICT Code of Conduct Committee**

**Composition:**

Coordinator of the Law and Information Technology Research Unit (chairman)
General Manager of the Personnel Department Directorate
Manager of the Staff Services General Management Directorate
Manager of the Communication Department
Manager of the KU Leuven Coordination Association
Manager of the Teaching and Learning Department
Manager of the ICTS Directorate (Information & Communication Technology & Systems)
Head of the Central ICTS Infrastructure Department
Head of the General Services for Education, Research, Communication and Cooperation Directorate
Staff Member Student Affairs
Group Manager Humanities and Social Sciences Group
Group Manager Science, Engineering and Technology Group
Group Manager Biomedical Sciences Group
ICTS Security Coordinator

**Responsibilities:**

- Responsible for the content and changes made to the ICT Code of Conduct
- Responsible for having changes to the ICT Code of Conduct ratified
- Responsible for notifying relevant users of these changes
- Analysing, approving and monitoring exceptions to the ICT Code of Conduct
ICTS Technical Unit

Composition:

Manager of the ICTS Directorate (Information & Communication Technology & Systems)
Head of the Central ICTS Infrastructure Department
Head of the Education, Research, Communication and Collaboration Facilities Department
ICTS Security Coordinator

Responsibilities:

- Analysing reports of violations
- Creating a file documenting the facts
- Providing this file to the HR General Manager and/or the Vice Rector for Student Affairs

Vice Rector for Student Affairs

Responsibilities:

- Analysing the severity of the complaint file
- Initiating a disciplinary procedure when necessary

Appendix: internal regulations and service provisions

- Internal regulations governing the use of the personal data of students and staff
  https://admin.kuleuven.be/td/fd/cld/persoonsgegevens.html
  Every applicant shall be considered to have familiarised him/herself with these regulations insofar as it concerns him/her and shall adhere to these regulations.


- Service provisions for the “Use of the personal data of students and staff”: https://admin.kuleuven.be/personeel/intranet/td/fd/cld/persoonsgegevens.html

- Service provisions for the “Protection of privacy”: http://www.kuleuven.be/bc/bpl_e.html

- Disciplinary measures: https://admin.kuleuven.be/personeel/intranet/regelgeving/reglement_n.html


- Service provisions 1999/01 dated 26/04/99: “Personal pages on the internet”
  https://admin.kuleuven.be/icts/intranet/dienstvoorschriften/persoonlijkepaginas


- Regulations on education and examinations: