UNIVERSITEIT GENT

POLICY FOR CORRECT USAGE OF THE UGENT ICT INFRASTRUCTURE[1]

(approved by the Executive Board on 19 May 2017)

(For definitions and terminology: check item 6 at the end of this document)

1. PERMITTED AND FORBIDDEN USAGE OF THE UGENT ICT INFRASTRUCTURE

1.1. The UGent ICT infrastructure can be used **for rightful activities that take place within the regular operation of Ghent University, in particular for research, education and service provision, and for activities in support thereof**. This implies the following (non-exhaustive list):

- Extensive usage for personal or recreational purposes is not permitted;
- The ICT infrastructure cannot be used for commercial activities, except when these are necessary for the regular operation of Ghent University;
- Each usage that violates the applicable legislative and regulatory framework is forbidden;
- The ICT infrastructure cannot be used to deliberately share confidential information[2] with receivers other than those who are entitled to it (unless permission has been given by the university board, for example related to a whistleblowers arrangement);
- It is only permitted to grant access to UGentNet to people who or systems that have been authorized by the university board;
- Violations of (security) policies or terms of use of internal or external IT systems are forbidden.

1.2. The ICT infrastructure cannot be used to share **unauthorized information**. Unauthorized information is considered to comprise (non-exhaustive list):

- Information that calls for racism, xenophobia, discrimination,…;
- Information that breaches public order or good morals;
- Offensive, defamatory of hurtful information;

[1] aka “Acceptable Use Policy”
aka “Rules for correct usage of the UGent network and the computers managed by DICT.”
[2] As defined in the policy document “Guidelines for the classification of information and data” (BC 10.7.2015), in anticipation of a broader debate on classification and confidentiality of information. https://www.ugent.be/en/facilities/ict/information-security/classification-data.pdf

- Bullying, hate mail or calls for violence

1.3. Users of the UGent ICT infrastructure have to respect the European and Belgian **privacy law**. This implies among other things that the privacy of users, in particular the confidentiality and integrity of their private data and the privacy of their communication, cannot be violated:
   - It is not permitted to read the emails in the personal mailbox of unshared files (especially those stored on the personal disk space or "home drive") of another user without their unambiguous permission.
   - Should data of a certain user be consultable by others, they should be stored on shared disk space or in a shared mailbox; or a different type of proxy functionality should be used.
   - Access to private data is only permitted in individual exceptions by court order or as requested by National Security.
   - Logging and monitoring of metadata of communication and access to related data is not determined in the present document. A specific policy document related to these issues will be drawn up.
   - Exceptional access to data of persons who are temporarily or permanently in legal incapacity (for example in case of a serious accident, coma or death, …) does not lie within the application area of the present document. A specific procedure will be determined to this end.

1.4. Users of the UGent ICT infrastructure have to respect **copyright and other intellectual laws.** This implies among other things that material and software protected by copyright cannot be shared or copied when that violates copyright laws or license terms.

1.5. It is only permitted **to install and use software** on equipment that is part of the UGent ICT infrastructure under these conditions:
   - all applicable conditions in terms of copyright and/or license terms are correctly satisfied, in other words the effective usage should be in agreement with the license terms (for example certain educational licenses cannot be used in a research context);
   - related information security risks were evaluated and deemed acceptable with due care, or were with due diligence reduced to an acceptable level (for example by safe configuration or security tests)[3];
   - should a user want to employ software that does not meet these conditions, an alternative has to be found that does satisfy these criteria.

1.6. It is forbidden to **breach the security** of the UGent ICT infrastructure, of systems connected to Belnet, other external IT systems and the Internet[4]. Examples of these breaches are (non-exhaustive list):
   - Forcing access to systems to which a user is not authorized or entitled (even though those systems may be insufficiently secured), as well as attempts thereto;
   - Circumventing internal and external system and network security;
   - Intercepting information meant for others, for example by capturing network traffic via a fixed network connection or with wireless equipment;
   - Pretending to be another user, for example by logging in and working with someone else's account data and without their permission (being understood that the user who

[3] https://www.ugent.be/en/facilities/ict/information-security/overview.htm
[4] See also the Belgian law of 28 November 2000 on IT crime.

deliberately shares their account data violates the information security policy (see 2.3));
- Ill-intentionally designing, installing, (attempting to) execute or (trying to) share malicious software (for example computer viruses) on the ICT infrastructure of Ghent University;
- Performing malicious actions that lead to partial or complete destruction of (confidentiality, integrity or availability of) IT data.

Note: Certain activities can be allowed for educational (for example practical classes) or research purposes within a clearly defined framework and on a restricted network that is not or not directly linked to UGentNet.

1.7. It is **forbidden to trace vulnerabilities** in the security of the UGent ICT infrastructure, even with good intentions (so-called ethical hacking).
- Exception: ICT administrators (both central and decentralized) should actively trace (or let someone trace) and remedy (or let someone remedy) vulnerabilities of systems and applications they are responsible for[5].
- Should a vulnerability in the security of ICT infrastructure of Ghent University be discovered (for example coincidentally), this has to be reported as soon as possible to the DICT help desk and to the appropriate administrator, developer or provider of said system. Exploiting or immediately revealing such vulnerabilities will be considered inappropriate.

1.8. **Systems that can connect to UGentNet**:

- Within the buildings of Ghent University, computers and other systems can connect to UGentNet via a UTP cable with an IP address that is assigned automatically or by DICT according to the existing procedures[6].
- To guarantee a proper functioning of the network, assigning fixed IP addresses and host names is centrally managed by DICT. Should there be changes to the registration data, these have to be reported to DICT by the responsible for the system (for example a new system is employed, a device with a registered IP number is no longer in use, a change in who is responsible has taken place,…).
- Both registered and unregistered systems (for example own devices such as laptops, smartphones, tablets) can wirelessly connect to the UGent ICT infrastructure via Eduroam[7] within UGent buildings.
- Both registered and unregistered systems (for example own devices such as laptops, smartphones, tablets) can use the UGent ICT infrastructure outside UGent buildings via Athena[8] or connect via VPN[9].
- In university halls of residence, students can connect their own systems via UTP cable without prior registration[10]. Certain limitations apply to these connections. Extensive functionality is possible via VPN.
- All systems using or connecting to UGent ICT infrastructure, both via cable and wirelessly, should be sufficiently protected in accordance with the UGent information

[5] http://www.ugent.be/en/facilities/ict/information-security/safe-system-administration.pdf
[6] http://www.helpdesk.ugent.be/ugentnet/en
[7] http://www.helpdesk.ugent.be/eduroam/en
[8] http://www.helpdesk.ugent.be/athena/en
[9] http://www.helpdesk.ugent.be/vpn/en
[10] http://www.helpdesk.ugent.be/ugentnet/en/studentenhomes.php

security policy[11]. Devices that do not satisfy these criteria (for example legacy systems that cannot be updated) should be disconnected from UGentNet.

- With a view to a proper functioning and security of the ICT infrastructure and in particular UGentNet, it is only allowed to change the structure of configuration of UGentNet with permission of the ICT functional domain. Installing extra active network components hence requires permission of the central ICT functional domain.
- The central ICT functional domain provides and manages all WiFi wireless connection points; installing own wireless access points is not permitted[12].

1.9. The functioning or the UGent ICT infrastructure relies on **limited means** in terms of storage capacity, computing power, bandwidth, supporting staff, etcetera. Therefore, these means have to be implemented **as efficiently as possible**:

- Limits established for mailboxes[13] or central desk space[14] have to be abided, which implies that the user clears redundant or obsolete mails and files (keeping in mind the costs and benefits of such actions), and organizes information in accordance with the principles of proper digital hygiene[15].
- It is forbidden to deliberately harm the proper functioning of the university network and other services and computers managed by DICT, for example intentionally overload the network or certain applications (so-called denial of service), or by sending unwanted emails to big groups of receivers (so-called spam). This paragraph forbids interrupting the proper functioning of the services of Ghent University, yet only in the technical sense – this paragraph does not address the issue whether or not such forms of mass communication are opportune.
- Efficient usage of the UGent ICT infrastructure requires that if possible the centrally provided infrastructure is addressed before the usage of decentralized infrastructure is considered. In the latter case, it is best to consult the ICT functional domain to check to which extent the required functionality is centrally provided or can be provided (possibly at a later stage). ICT projects of more than 30.000 euro should in principle be presented to the ICT Commission of Ghent University.

2. RESPONSABILITIES OF THE USERS

2.1. Users with a **UGent account[16]** gain access to the UGent ICT infrastructure by means of a user name and password[7]. The UGent account is an important part of the digital identity of the user and has to be carefully protected in accordance with the information security policy ofGhent University and in particular the accompanying practical guidelines[17].

2.2. A **personal UGent email address** is linked to the UGent account. This email address is the official channel of communication between the user and Ghent University. The user has to consult the corresponding mailbox on a regular basis.

---

[11] https://www.ugent.be/en/facilities/ict/information-security/overview.htm
[12] By decision BC 13 May 2004, exceptions are thus only possible by decision of the university board.
[13] http://helpdesk.ugent.be/email/en/
[14] http://helpdesk.ugent.be/netdisk/en/
[15] http://www.ugent.be/nl/univgent/collecties/archief/informatiebeheer/informatiebeheer-2-digitale-hygiene
[16] http://helpdesk.ugent.be/account/en/
[17] http://helpdesk.ugent.be/account/en/wachtwoord.php

2.3. A UGent account is strictly personal. The user is responsible for the assigned account and for what happens while using it, unless the user has fallen victim to abuse of their account in spite of due care. In accordance with the information security policy, the following rules, among others, have to be taken in to account for the protection of the UGent account[18]:

- A strong password (or a strong password sentence[19]) has to be selected, which should be altered at least once a year[20].
- The password has to be kept strictly secret. Log-in data of the own account cannot be passed on to others, not even to close colleagues. Should there be applications that others have to be able to use on behalf of the user, this has to happen via a proxy-functionality.
- Should the password be presumed to have become known, the compromised password has to be changed immediately[21].
- It is forbidden to use the same password of a UGent account for other internal or external services.
- It is not permitted to let others work via the personal account. Should a violation of this rule not be avoidable for practical reasons, an exception can be temporarily tolerated in anticipation of a correct solution. These exceptions should be reported to the information security counsellor in advance. Staff members or students cannot be obliged to share their account data.
- When a computer is left unattended, even if only for a short while, it should be locked or signed off. This holds for computers managed by DICT (for example computers in auditoria, computer classes or public desktops) as well as for own and other devices.

2.4. The ICT infrastructure provided by Ghent University should be treated with **due care** by its users. This entails among other things:

- When a user notes a failure or malfunctioning of a part of the ICT infrastructure, this should be reported to the responsible ICT administrator or to the DICT help desk.
- UGent ICT devices cannot be left in an irresponsible way and thus exposed to the risk of theft or abuse.
- In accordance with the practical guidelines of the information security policy, all users and ICT administrators should take responsibility for the protection of the provided ICT infrastructure.
- All incidents related to information security (for example abuse of an account, infection with malware, theft of a device or data, a data leak with personal data or confidential information – non-exhaustive list) should be reported to the DICT help desk[22] as soon as possible.

3. RESPONSIBILITIES TOWARDS SERVICE PROVIDER BELNET

[18] Non-exhaustive enumeration and in anticipation of possible extra security measures, for example 2-factor authentication for critical applications and critical accounts.
[19] https://www.safeonweb.be/nl/tips/wat-je-moet-weten-over-het-veiliger-maken-van-wachtwoorden
[20] This is also technically enforced, in accordance with decision BC 11 December 2015
[21] https://password.ugent.be
[22] http://helpdesk.ugent.be/extra/en

The university network UGentNet is linked to Belnet[23], the Belgian research network. Belnet has an Acceptable Use Policy ("AUP")[24], which co-determines what is (not) permitted on networks linked to Belnet.

Belnet endorses the Code of Conduct for Service Providers[25] of the Belgian Internet Service Providers Association (ISPA), and the Belgian cooperation protocol for combatting unauthorized conduct on the internet" ("Samenwerkingsprotocol ter bestrijding van ongeoorloofd gedrag op internet"). Wireless WiFi access UGentNet via Eduroam falls under the conditions of the agreement for joining the Eduroam service of Belnet ("Overeenkomst voor toetreding tot de Eduroam dienst van Belnet")[26].

4. COMPLIANCE

By accepting an account or using the UGent ICT infrastructure, users bind themselves to complying with these regulations. This policy thus also holds for external users of Eduroam via UGent access points.

5. SUPERVISION, MONITORING AND SANCTIONS

5.1. The UGent ICT infrastructure is checked (logging and monitoring) by the ICT system administrators to ensure a proper functioning and detect and prevent abuse. The level of detail of logging and monitoring cannot be higher and the storage time cannot be longer than necessary to the specific purpose.

Supervision and monitoring happen in accordance with the collective labour agreement CAO 8[27].

5.2. The information security counsellor of Ghent University has monitoring authority for the safe processing of personal identifiable data at UGent.

5.3. Incidents should be reported at the DICT help desk, which functions as the first contact point and referral point to other authorized parties such as the information security counsellor.

5.4. In case of incidents, DICT can decide to take technical preventative measures with the sole purpose of protecting the ICT infrastructure and its proper functioning.

5.5. Considering the severity of the violation, possible measures and sanctions that can be taken against persons when detecting active, intentional and repeated violations of this policy are:

- Disciplinary measures taken by the Chancellor: temporary cancellation of an account or temporary restriction of access to (parts of) the ICT infrastructure (in which case a balance is to be found between the importance of the service, the protection of the

[23] http://www.belnet.be
[24] See the Acceptable Use Policy ("AUP") of the BELNET internet services, version 01.02.2012
[25] http://www.ispa.be/code-conduct-nl
[26] See the agreement for joining the Eduroam service of Belnet.
[27] https://www.privacycommission.be/sites/privacycommission/files/documents/cao-081.pdf

systems and the rights of the concerned persons, as the account is often necessary in the context of the job or studies);
- Measures and sanctions as provided in the applicable legal framework (for example labour law) and in the internal guidelines of Ghent University, such as disciplinary policies.

6. DEFINITIONS

6.1. **ICT-infrastructure**: this means both the network infrastructure and other physical IT-related devices owned or used by Ghent University (data centers, servers, storage, desktops, printers, telephony, ...). All internal and external ICT applications and services owned or commissioned by Ghent University are also considered part of this policy. This includes amongst other things the services for remote access and remote use (for example Athena or VPN) and services for wireless connection as part of Eduroam.

6.2. **UGentNET**: the UGent computer network managed by DICT (the central Information and Communication Technology functional domain) and all its active and passive components.

6.3. **ICT-administrators**: all responsible persons for maintenance and proper functioning of the ICT infrastructure, both central (linked to DICT) and decentralized (linked to faculties and university services)

6.4. **Authorized user**: Each person who can use the UGent ICT infrastructure. A distinction can be made between:
- users with a regular UGent account[28] (students, staff members and volunteers of Ghent University, registered visitors at Ghent University, ...)
- users of Eduroam without a UGent account, but with an account at a different institution that is connected to Eduroam
- users with a temporary UGentGuest account for WiFi
- other users that are granted specific access based on decisions by the general management of the UGent.

[28] http://helpdesk.ugent.be/account/hoe.php
Decisions of the general university management in relation to granting UGent accounts (non-exhaustive list):
- BC 20 September 2007: UGent accounts in general
- BC 28 February 2008: accounts for exam contractors and retired administrative & technical staff
- BC 11 March 2010: accounts for career breakers and annual extension or retired persons
- BC 16 December 2010: accounts for visitors and external VSC users
- BC 27 October 2011: accounts for external education provider, IVPV only when present in OASIS, limited
- account UCT, arrangement for integrated staff
- BC 27 September 2012: “mini-accounts” OASIS for re-registration, arrangement for integrated students
- BC 24 April 2014: deleting of accounts for Degree holders, full account UCT

About this text:
This is a translation of the original policy text in Dutch as approved by the management of Ghent University, (decision BC 19.05.2017) and published on https://codex.ugent.be?regid=REG000157.
In case of discrepancies or doubts about the interpretation of this text, the original Dutch version prevails.