Πανεπιστήμιο Κύπρου
University of Cyprus

COMMITTED TO EXCELLENCE EFQM

Please note that the English translation of the present Policy is for information purposes only and is not intended to have any legal effects. In the event that a dispute should arise about the interpretation of the information contained herein and the information contained in the original Greek document, the latter shall prevail.

ACCEPTABLE USE POLICY

ON INFORMATION AND COMMUNICATION TECHNOLOGY

SERVICES AND SYSTEMS

In accordance with the applicable national, EU, and international legislation, and taking into account the need to establish a policy that determines the core and general policies governing all uses of Information and Communication Technology services, systems, and resources, as well as the access to external networks and web resources, which are provided and managed by the Technical Support Teams, the IT Infrastructure Service or other organisational entities of the University of Cyprus, the ad hoc Committee

DREW UP

The present **Acceptable Use Policy on Information and Communication Technology Services and Systems**.

All members of the University Community (including Academic and Administrative staff members, students, researchers, and authorised visitors) are expected to be familiar with and comply with this *Policy*. **The use of Information and Technology services and systems shall imply acceptance of the *Policy***.

The present **Acceptable Use Policy on Information and Communication Technology Services and Systems** complies with the applicable national, EU, and international legislation. In particular, the following legislation has been considered:

i. The Constitution of the Republic of Cyprus and the European Convention on Human Rights (ECHR);
ii. The University of Cyprus Law N. 144/1989, as subsequently amended, as well as the relevant Regulations and Rules;
iii. The General Data Protection Regulation (EU) 2016/679 and the relevant Directives of the Commissioner for Personal Data Protection;
iv. The Retention of Telecommunication Data for the Purpose of Investigation of Serious Criminal Offences Law of 2007 (N. 183(I)/2007);
v. The Protection of Private Communications (Interception of Communications) Law of 1996, N. 92(I)/1996;
vi. The Convention of the Council of Europe on Cybercrime (Ratification) Law of 2004;
vii. The Criminal Code, Cap. 154;
viii. The Civil Wrongs Law, Cap. 148;
ix. The Regulation of Electronic Communications and Postal Services Law of 2004;
x. The Intellectual Property Rights Law N.59/76;

xi. The Trademarks Law, Cap. 268;

xii. The Patents Law of 1998, N. 16(I)/1998;

xiii. The Law of 2004, N. 156(I)/2004 on Certain Aspects of Information Society Services, in particular Electronic Commerce, and Related Matters.

1. INTRODUCTION

1.1. Policies

The present document, hereinafter referred to as the *Policy*, summarises the core and general policies applicable to all uses of Information and Communication Technology services and systems. All Information and Communication Technology (ICT) services, systems, and resources will hereinafter be referred to as *Information Technology (IT)*. Any organisational entities seeking to establish specific policies for the use of the services and systems they provide and manage should first approach the Information Systems Committee to ensure that said policies comply with and do not contradict the *Policy*. (Any such policies that are approved will be included in future versions of the *Policy*.)

These policies are governed by the general legislation and the Laws, Regulations, and Rules of the University of Cyprus. Therefore, for example, provisions on issues concerning (intellectual and industrial) property, privacy, and publication in an ordinary way apply to said issues when i) computers and mobile devices are involved, ii) they concern the use of (or publication via) the Global Information Grid or the Internet, message boards or other similar messaging platforms (such as Wikipedia and various wikis, social networks, and chat rooms, or iii) text, or audio-visual and/or audio material or files are included in or attached to electronic messages.

1.2. Obligation to Comply

The *Policy* is binding on all users of Information Technology, without exception. Failure to comply with the *Policy* may result in suspension or, in particularly serious cases, termination of the provision of Information Technology services.

1.3. Policy

The Policy aims to ensure the smooth operation of Information Technology and to serve the mission of the University of Cyprus. Some of its provisions derive from the legal obligations of the University of Cyprus or are necessary for complying with its agreements with external parties or to comply with its legal obligations.

1.4. Clarification.

The University of Cyprus acts as the “carrier” of information through electronic channels rather than the "publisher" of information or the "publisher" or the source of the information content. Therefore, the

University of Cyprus should not be expected to have knowledge of and/or be responsible for the material or the communications that its Members i) send, share or publish through messaging systems such as email, through the Global Information Grid, Online Discussion Rooms or social networks or any other similar means of communication that may be developed, (ii) make available through any method of sharing data files. However, under certain circumstances, the University of Cyprus will be required to respond to formal complaints regarding such material and communications (See Chapter 5).

1.5. Comprehensiveness and Revisions

Apparently, it is impossible to systematically record and include all cases of unacceptable use of *Information Technology* in a single policy. Common sense and critical thinking alone suffice to evaluate new cases as unacceptable. Periodic revisions of the *Policy* are expected to keep it in line with developments in *Information Technology*.

1.6. Scope

The *Policy* concerns the use of *Information Technology*, including access to computer systems and equipment (e.g. microcomputers, laptops, mobile devices, servers, printers, software, network services, databases, electronic publications, etc.), online access to the Library and its systems, access to the telephone and voice mail systems, and access to the Internet.

The *Policy* shall apply to (i) equipment and systems owned by the University of Cyprus, but also to personal equipment (owned by Members or authorised visitors and which makes use of the University network and resources), (ii) services and systems provided and managed by the IT Infrastructure Service or the Technical Support Teams in other organisational entities, such as the Library, (iii) services installed on the personal equipment of students or authorised visitors that is temporarily or permanently connected to the University network, (iv) any other systems that obtain an authorised connection and connect to the University network using Internet addresses assigned to the University, (v) actions initiated from computer systems or mobile devices maintained or used outside the University by members of the University Community, which are, however, remotely connected to the University network.

The *Policy* shall also apply to the actions of visitors to the University of Cyprus who use the service of temporary access to the wireless network of the University or register their personal equipment through University Services to use the University network. (Such personal equipment, which is attached to or connected through equipment or resources of the University, shall be subject to the same regime as the University of Cyprus equipment.)

1.7. General

In general, harassment or inappropriate conduct through *Information T*echnology is a typical case of unacceptable use and shall be assessed as appropriate in terms of its severity.

Violation of the Policy shall constitute a disciplinary offence and shall be dealt with according to the applicable disciplinary procedure.

2. ACCEPTABLE USE

As a general principle, acceptable use of *Information T*echnology is defined as the use made for purposes related to the work and mission of the University. Personal and/or non-official use may be made under certain circumstances, but shall be kept to a minimum so as not to create additional costs to the University and not interfere with the use of resources (e.g. shared bandwidth or printers) for administrative purposes.

2.1. Proper Use

Communication using *Information Technology* (e.g. composing, sending or forwarding electronic messages, creating and publishing announcements on the Global Information Grid or email lists, promoting and submitting photocopied or video material for electronic transmission, etc.) shall be expected to be respectful of the recipients.

In particular, sending, communicating or displaying, or causing or facilitating the sending, communication or display, of threatening, harassing, abusive, or defamatory messages or postings against another person shall be prohibited. The intentional use of anonymity or pseudonymity in electronic communications for unlawful purposes shall also be prohibited.

When sharing information, users should be respectful, sensitive, and discreet; in particular, they should avoid sharing, displaying publicly, or showing inappropriate images, sounds or messages that could create a bad atmosphere for or harass others.

2.2. Respecting the Reputation of the University

Users shall be expected to respect the principles, values, and mission of the University of Cyprus when using *Information Technology*. Any misuse of the name of the University of Cyprus shall be prohibited.

2.3. *Policy* Awareness

Users shall be aware of, accept, and implement the *Policy*. They shall also exercise good judgment in cases not covered by the Policy.

2.4. Use as a Personal Privilege

The use of *Information Technology* is a personal privilege and may not be extended or transferred to third parties without authorisation. (This includes granting network services to others by transferring the network connection provided).

2.5 Responsibility of *System Administrators*

System Administrators shall be appointed as responsible for taking all reasonable and, under the circumstances, legal measures to record, manage, and protect the University's Information Technology assets, as well as for the proper implementation of the management of *Information Technology* and licensing agreements, and for safeguarding the reputation of the University from any damage that may result from a breach of the *Policy*. They shall also take all appropriate measures to ensure that copyrighted *Information Technology* material (such as software, movies, music, and computer games) is not reproduced, published, distributed to or otherwise used by third parties without the authorisation of the intellectual and industrial property right holder.

2.6. Incident Reports

Users shall be expected to report without delay to the appropriate System Administrator and/or University Supervisor/Officer any reasonable suspicion of an offence committed through or involving *Information Technology* equipment, services, or systems. The recipients of the report shall maintain absolute confidentiality and respect the privacy and individuality of all persons involved (see Chapter 5).

3. OBLIGATIONS AND BEST PRACTICES

3.1. Electronic Data Management

3.1.1. Personal Data

In general, the storage and management of electronic information shall follow the practice of recording, maintaining, storing, and managing paper information. Protecting personal data such as student records, academic transcripts, medical data, and other personal information protected by the applicable law shall be imperative. Provided that, the use and any processing of personal data shall be carried out only for specific, legitimate purposes and solely for the purposes of the University of Cyprus. It is necessary to ensure that the confidentiality of communication and privacy are protected.

3.1.2. Data Erasure

When replacing or handing over electronic equipment/devices, all data shall be deleted from the device.

3.1.3. Electronic Mail

Users shall take all appropriate measures to avoid causing problems to the smooth operation of the email system. (For example, it is also advisable to periodically clear the "inbox" and "sent" folders in the email systems and archiving applications to keep emails small.)

For greater protection and easier management of data concerning the University of Cyprus, the communication and/or circulation of information on official matters shall be carried out through corporate electronic accounts instead of external accounts. Users shall be advised to exercise due diligence to identify misleading, malicious or forged emails that seek to extract personal or security information and/or damage computer systems. In the event that such messages come to the attention of users, they shall ignore and delete them.

3.1.4. Email Address Format

Administrative and Academic staff, students, and guest accounts have the following email address format:

[Surname.First Name]@ucy.ac.cy

And in case this email address is already used by another user:

[Surname.First Name.Serial Number]@ucy.ac.cy

Administrative and Academic staff, students, and guest accounts also have an additional pseudonym in the following format:

[username]@ucy.ac.cy

3.1.5. Duty to Protect

Users shall ensure that backups are maintained for important files stored on personal equipment that is not subject to automatic backup. They shall also ensure protection against unauthorised access to classified information or to works and other items which are protected by intellectual and industrial property rights and are stored and/or installed on their personal equipment.

In general, it is not advisable to submit sensitive or confidential information on portable devices (e.g. USB, laptops, smartphones, etc.). Where this is inevitable, it is advisable to encrypt the information so that it cannot be accessed by unauthorised persons, in case the portable device falls into their hands. In this case, it is also appropriate to provide adequate physical protection for the mobile device.

If unauthorised access to a personal account is observed, either due to theft or loss of a portable device (e.g. USB, laptops, smartphones, etc.) or due to any kind of security breach of the system, the member who possessed the mobile device or becomes aware of the security breach shall immediately inform the competent authorities (e.g. the Chairperson of the Department, the Head of the Section, the Head of the Department etc.).

Users shall be advised to exercise due caution when storing files containing sensitive or confidential information on cloud storage services.

3.2. Network and Information Security

3.2.1. Account Protection

All members of the University Community shall be **accountable** to the University for the **personal and/or official account** provided to them and shall be **responsible** for all actions taken on that account.

Each member shall be expected to take reasonable measures to prevent others from using the account. The password of an account shall be considered confidential; its disclosure to third parties shall be prohibited, and its protection shall be required. The initial password provided at the time of opening the account shall be changed, and strong passwords shall be chosen. It is also recommended that the password be changed periodically, in accordance with the instructions provided by the IT Infrastructure Service at the time. In particular, unauthorised users may not disclose the password of an **official account**.

Likewise, security questions, digital certificates, as well as similar passwords of any kind that may be used to provide secure access, shall also be protected.

It is recommended that official records be kept separate from personal records.

3.2.2. Protection of Personal Information

It is recommended that personal information (e.g. account passwords, PIN codes, credit card numbers etc.) not be stored in accounts, systems, services, and/or websites of the University of Cyprus.

3.2.3. System Security

Specifically, the System Administrator shall be responsible for the proper and secure operation and protection of the systems under his/her responsibility, as well as for the safe protection of the root or administrative password of the system. He/She shall be also responsible for the installation and maintenance of protective mechanisms (e.g. anti-virus software, firewalls, and back-up system).

3.2.4. Protection of Applications on the Global Information Grid

The administrator of each server or application on the Global Information Grid that operates within the University Network shall take all appropriate security measures, in accordance with the best practices and the applicable security policies.

3.2.5. Reporting Security Gaps

All users shall immediately **report** to the competent System Administrator or the competent authorities any security gap in the computer systems or the network that comes to their attention. Provided that, the exploitation of such security gaps in any way shall be **prohibited**.

3.3. Use of Shared Resources and Services

Provided that, Information Technology is intended to be used for activities that promote the educational and research purposes of the University, such as teaching, independent study, authorised and independent research, and the official work of the Departments, Faculties, Services, Research Units, Centres and other Organisational Entities.

3.3.1. Performance

The IT Infrastructure Service and the Technical Support Teams shall have full authority and responsibility for taking all actions necessary to ensure an acceptable level of performance and prevent any unnecessary, excessive, or inappropriate use of resources that could cause service disruption. Users shall decide in advance for those cases where the use of resources could disrupt the normal operation of the systems.

3.3.2. Library Resources

Many of the databases, e-journals and other publications provided by the Library shall be subject to Licence Agreements with external suppliers that impose restrictions on their use. (For example, there may be restrictions on the number of texts that can be accessed or the number of pages that can be printed.) Library users shall be informed of such contractual and technical restrictions and shall be prohibited from violating them or attempting to violate them. Violation of the restrictions may result in the cancellation of the Licence Agreement and termination of access to the resources. Therefore, violators shall be subject to disciplinary

action and/or possible criminal prosecution, while the University of Cyprus shall reserve the right to claim compensation for damages that may arise from the violation and/or cancellation of the agreement.

3.3.3. Access to the Internet and the Wireless Network

Any abuse of service that hinders the provision of Network Services may result in the temporary or permanent exclusion of the device connected to the network.

3.3.4. Sending Harassing Messages

As a general rule, bulk emails that may lead to email system disruption shall not be allowed. For sending bulk emails, it is advisable to use the tools available. Finally, repeatedly sending multiple messages to a user or groups of users ('bombing') shall be prohibited. Spam, harassing and malicious emails shall be prohibited as well.

3.3.5. Sparing Use of Resources (Storage, Transmission, Printing, Sharing)

It is inadvisable to store excessive amounts of data on central or departmental computer systems and to run programmes requiring a large number of resources (e.g. memory, time, etc.) when there are more efficient programmes. (The authorised use and execution of such programmes for educational or research purposes is excepted.) Running servers or daemons on shared systems shall be inadvisable.

Transmitting excessive amounts of data over the University's network when it is not necessary shall also be inadvisable.

Printing should be done sparingly and only when the text to be printed cannot be shared electronically in an efficient manner. Duplex printing and the printing of multiple pages on a single sheet of paper shall be preferred. No paper shall be removed from any department/service/entity printers for any other purpose.

Moreover, the effective shared use of the minimum number of copies of the same software, for which the purchase of a licence is required, shall be pursued.

3.3.6. Shared Workstations/Machines

Shared workstations/machines shall be available for academic activities. The use of shared machines for activities not related to University purposes shall be avoided.

Authorised access shall be required to use a shared workstation/machine. The unattended execution of processes on a machine or the unauthorised placement of signs to indicate that a machine is “occupied”, or “locking” a shared machine, shall be prohibited, as these actions prevent others from using the machine. The machine user may not be absent for more than a few minutes. A machine left unattended for more than

fifteen minutes will be assumed to be available for use, and any process running on it may be terminated without warning.

3.4. Network and Systems Operation

3.4.1. Ungranted Privileges

Obtaining or attempting to obtain ungranted network or system privileges and obstructing or impairing such privileges shall be prohibited. In particular, any action that impedes the supervision and control of computer systems deriving from such privileges shall not be permitted. Creating and executing any code that periodically interrupts or interferes with the computer systems and services, as well as using sniffer programmes for identifying technical gaps in the systems, shall also be prohibited.

3.4.2. Interference with Information Transmission

Any attempt to receive, capture, intercept, modify, or reject information or to interfere in any way with its transmission on any University network shall be prohibited.

3.4.3. Unauthorised Sending of Electronic Messages

In general, the use of programmes, scripts or other similar means to send unauthorised electronic messages shall be prohibited.

3.4.4. Wireless Network Operation

The installation of a wireless access point in any University premises (including rented premises) can only be carried out with the approval of the competent authority managing the wireless network.

Any interference with the University's wireless networks shall be prohibited.

3.4.5. Equipment Connection

The installation of network equipment (e.g. routers, switches, wireless access points, etc.) and other equipment, as well as their connection to the wired network, shall be performed under the supervision of the Manager of the relevant Network (e.g. Networks Sector of the IT Infrastructure Service, Technical Support Team of the Department of Computer Science). At the time of registration, accurate details of the equipment shall be provided.

The unauthorised use of IP addresses on the University of Cyprus network and the creation of false (static or dynamic) IP addresses shall be prohibited. The unauthorised installation of servers that improperly assign IP addresses on the University network shall also be prohibited.

If any interference from an electronic gadget (e.g. cordless phone) is detected, the owner of the gadget may be required to take appropriate action to terminate the interference.

4. UNACCEPTABLE USE

Unacceptable use of *Information Technology* shall be defined as the use that is not related to the purposes or mission of the University. Such uses include, but are not limited to, the following:

4.1. Commercial Use

4.1.1. General

The use of *Information Tec*hnology (including resources and services) for **commercial activities** not related to the University of Cyprus shall be prohibited.

In particular, organisations/entities/associations hosted by the University of Cyprus must use other (electronic) resources and services for any of their (commercial) activities that are not related to the University of Cyprus.

4.1.2. Links to and from Commercial Websites

Any links from an internal website to a commercial website shall be accompanied by a note stating that the content is not supported or endorsed by the University of Cyprus. Specific approval from the relevant organisational entity shall be required for the creation and maintenance of an external website that appears as a University of Cyprus website and for the creation and maintenance of an internal website that represents an external group or activity that is not affiliated, related to, or formally associated with the University of Cyprus.

Unauthorised use of the University of Cyprus email or website, or electronic lists for campaigns, including but not limited to advertising campaigns and fundraisers, shall be prohibited.

4.3. Use for Political Purposes

Members and/or groups of the University community who use University resources and services for political purposes shall specify that the views they express are **strictly personal**.

No statements for or against political parties or candidates for public office may be published on the University of Cyprus website.

Any links from an internal website to websites of political parties or candidates for public office shall be accompanied by a note stating that their content is not supported or endorsed by the University of Cyprus.

5. PRIVACY

5.1. Respect for and Assurance of Privacy

The University of Cyprus respects and takes all reasonable measures, within its means, to ensure the privacy of all members of the University Community within the scope of the *Policy*, as defined by the Constitution, the EU acquis, the International Treaties, and the National Legislation.

Unauthorised access to the personal equipment, personal account or private communications of members of the University Community shall be prohibited. If any person inadvertently gains such access, they shall immediately terminate it and notify the affected person.

Unauthorised access (see 5.1.3) to the content and external data of phone calls, fax, voicemail and electronic mail of members of the University Community shall be prohibited.

5.1.1. Private Communication

The University of Cyprus respects the **confidentiality** of *Private Communication*.

Private Communication shall be defined as any online communication, wired or wireless, through *Information Technology*, carried out by a person under circumstances that allow them to reasonably expect that their communication will not be intercepted or monitored by any person other than the intended recipient.

5.1.2. Electronic Records

Unauthorised access to the electronic records of University Community members shall be prohibited.

In particular, any action to retrieve, access, search, copy, use, modify or delete electronic texts, files, codes, images, films, music or audio files and programmes without authorisation shall be prohibited.

5.1.3. Waiver of Confidentiality

Confidentiality may be waived pursuant to a court order by the authority competent under the Law and in accordance with its terms; the University of Cyprus shall be obliged by Law to comply with said terms.

The waiver of confidentiality may entail access to Private Communication, personal equipment, and the content of electronic records.

5.2. Availability of and Access to Official Electronic Records

Where appropriate, and for the purposes of cooperation and proper functioning, members of the University of Cyprus shall be required to make any official electronic records they hold available to other University members.

Administrative Staff members who hold official electronic records on personal equipment or on a personal account, which may be required at any time for the proper functioning of the University, shall ensure that the Head of the Organisational Entity can access them in their absence. In the event that this is not ensured in advance, the necessary access shall be arranged by the System Administrator of the Organisational Entity in the presence of the Head of the Organisational Entity or their representatives, who shall take all necessary measures to fully respect and ensure Privacy.

Access shall be permitted only in exceptional cases of extreme urgency, provided the records cannot be made available within a reasonable time by the Administrative Staff member who holds them, and provided that every effort has been made to inform and make them available beforehand; access to all other records shall be prohibited.

5.3. Obligations upon Staff Departure

Upon the departure of an Academic Staff member, or a Special Teaching Staff member, or an Administrative Staff member, the member shall be required to **delete** any **personal** files, as well as any electronic and voice messages stored on the IT equipment provided to them, and return said equipment.

Their personal account shall be deleted within six months of their departure or within one month of their resignation/termination, unless a request for deferment of the deletion is submitted and approved by the

Head of the relevant Organisational Entity. The personal accounts of students or other categories of staff (e.g. Visiting Faculty, Special Scientists, etc.) shall be deleted within three months of their graduation, departure, or removal. Email addresses of retiring staff may be retained for life, at the request of the person retiring. In exceptional cases, and with the approval of the Rector's Council or the Director of Administration and Finance, an account may be deleted immediately, without any grace period.

Administrative Staff members who depart or are transferred to another Service/Department/Organisational Entity shall not delete or alter any official records and electronic messages they have received or sent in their official capacity or have created during their employment at the University. Said records shall be made available to their Immediate Supervisor, in accordance with the instructions received prior to their departure or transfer.

5.4. Provisions in the Event of Death

In the event that the deceased member maintained official electronic records on personal equipment or a personal account which are essential for the proper functioning of the University, access to said records may be permitted if they cannot otherwise be retrieved. Provided that, respect for Private Communication shall apply to this case also, while access to all other records shall be prohibited. Such access shall be arranged by the System Administrator of the Organisational Entity in the presence of the Head of the Organisational Entity and the Director of Administration and Finance or their representatives.

Upon the lapse of two years from the death of a University Community member, their personal account along with any electronic records, as well as any electronic and voice messages stored on the IT equipment provided to them, shall be deleted. However, instead of the deletion mentioned above, Members shall always reserve the right to choose either: to have their electronic records and their electronic and voice messages, as previously stated, become part of the University Archive, in accordance with the applicable Law and the Records Management Policy of the University at the time, or have them reach the Trustee of their property to be appointed or any other person the Member may appoint. Provided that, this right may be exercised at the time of opening the personal account or at any time thereafter.

6. INTELLECTUAL AND INDUSTRIAL PROPERTY

The University of Cyprus shall respect and take all reasonable measures, within its means, to safeguard intellectual and industrial property, in accordance with the applicable national, EU, and international legislation.

Infringement of intellectual or industrial property rights through the use of *Information Technology* shall constitute a disciplinary offence, which, if detected, may result in the temporary suspension of the respective service or, if repeated, may lead to the deprivation and/or loss of the right to use *Information Technology*.

In particular, reproducing, publishing, reusing and/or further promoting, or otherwise making available to the public others' works or other protected items (including computer programmes, databases, multimedia works, etc.) shall be prohibited without the authorisation and/or due acknowledgement of the author and/or of the other right holder and/or without the required acknowledgement of the use. Specifically, only uses covered by exceptions/limitations to intellectual and industrial property rights, which comply with the agreed

conditions of purchase, licensing and/or use in accordance with the applicable legislation, shall be permitted. Provided that, in the latter case, the code of conduct for academic integrity shall apply accordingly for acknowledging and citing sources.

Revised on 4/12/2020

Information Systems Committee Meeting No. 7/2020