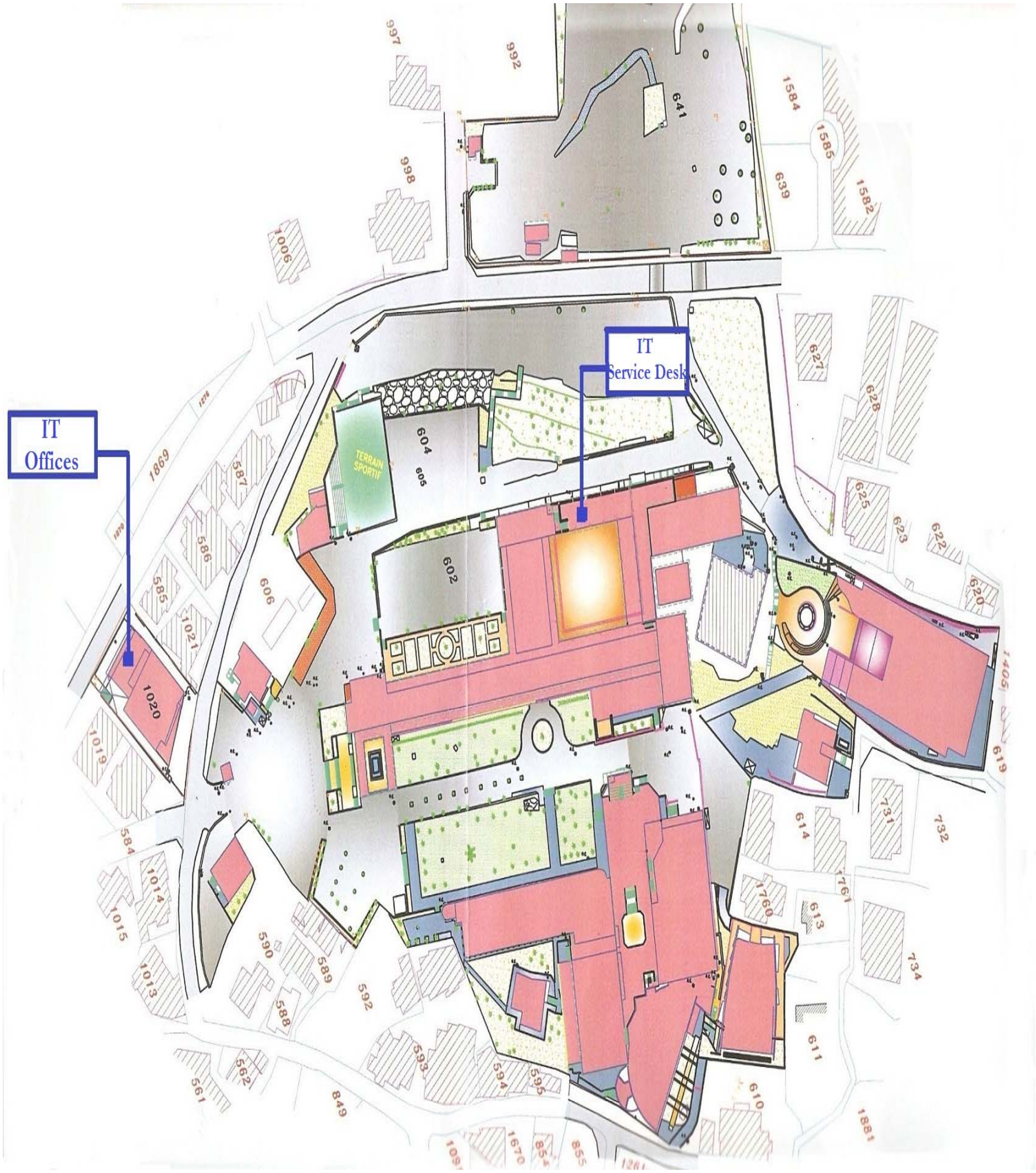
ICT Service Catalogue

Reference Guide

Student guide to IT services


IT
Offices
IT
Service Desk
TERRAIN
SPORTIF
997
992
641
1584
1585
1582
639
998
1006
627
628
604
605
1869
587
625
623
622
620
602
586
606
585
1021
1020
1406
619
1019
731
732
614
584
1014
1761
1760
613
1015
590
589
734
1013
592
588
611
593
562
594
595
561
849
610
1881
1670
854
855

Introduction:

Welcome to the student guide of ICT services in the Holy Spirit University of Kaslik. The following guide will give you an introduction to the IT facilities available, the information you need and places to go to get further help. Furthermore, your obligation as a student using IT services are mentioned.

Policy Statement:

Below is a summary of USEK policy, which will guide students using available resources. It is strongly recommended that students read the full policy.

1. Acceptable use of the University computer/network resources includes only those activities associated with college courses, programs and services; i.e. the University's mission in general.

2. It is the University's policy to provide access to the internet and email service, to facilitate reliable communications and to provide direct access to readily available sources of information for research, learning and academic needs.

3. In particular, the use of the internet, as a valuable tool and source of information, is acknowledged.

4. Students at USEK must protect:
   - Their Identity card (MACard) from being used by other individuals.
   - Their privacy of account and electronic information.

Acceptable Use:

1. USEK's students will be able to use the University computer facilities for the purposes of their academic studies.

2. The University provides electronic communication systems and services to all students, in support of its academic mission. The use of these facilities is subject to limitations necessary for the reliable operation of the electronic communication systems and services.

3. The electronic resources should be used solely for the intended purpose.

4. Students must respect the rights, privacy and property of others.

5. Students must adhere to the confidentiality rules governing the use of passwords and accounts.

6. Students of the University may use the computing facilities provided. Modest use, for private non-academic purposes, is usually acceptable.

7. Students must comply with all applicable laws.

Unacceptable Use:

1. Students must not attempt to gain access to any computer system or material, for which authorization has not been given.

2. Students may not use another individual's account, or attempt to crack or guess other users' passwords.

3. Intentional creation, execution, forwarding or introduction of any viruses, worms, Trojans or software designed to damage the performance of the University network is forbidden.

4. Students must not connect any computer device to the University network.

5. The corruption or destruction of other user data is forbidden.

6. Students must not engage in any activity considered wasteful of resources, such as playing computer games.

7. Any activity which may reflect adversely upon the University is forbidden.

8. Students must not download, store and disseminate copyrighted materials, including software and all forms of electronic data, without the permission of the holder of the copyright, or under the terms of the licenses held by the University.

Code of Ethics in IT Classrooms or Labs:

1. Food and beverages are prohibited in a computer environment. Both can damage computers. Please respect the cleanliness of USEK's labs and classrooms and help maintain the high standards of quality that IT offers.

2. Students must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities.

3. No equipment should be moved from its designated place, or be tampered with in any way, such as changing workstation characteristics.

4. Students should not act so as to deliberately or recklessly overload access links or switch equipment.

A. Username and Password

Each student is assigned a unique ID, username and password to be used on any system that resides at USEK facility; wireless, e-learning, banner, labs, EZproxy, electronic email.
Passwords are a critical part of information and network security.

Strong passwords promote a secure computing environment; badly chosen passwords endanger the information that they are supposed to protect.

Choosing a password:

- Passwords should contain a mixture of lower and upper case letters, numbers and other characters such as punctuation marks and symbols.
- They must include at least one numerical character.

Passwords should not

Contain names, word (that can be found in dictionaries), words in reverse order, abbreviations, acronyms or dates of birth.

Passwords must NEVER be disclosed to others. Do not allow other people to use your access unsupervised, as you will be held responsible for their actions.

Users must guard against responding to emails asking them to provide their username and passwords for system maintenance. These emails are fake and are a clear attempt to steal a user's identity for disreputable purposes.

Access rights and passwords:

1. Your access rights to the University's information systems are granted for your personal use only.

2. Students usually log in to the University's services and systems with their username and password:

- Same username and password for wireless, e-learning and windows login (username: Student ID)
- Student ID and password for banner.
- Email access.

3. You are held responsible for all the activities occurring under your user account. Do not reveal your username and password to others.

4. USEK employs a smart card (MACard) for identification and access control, as well as purchasing and printing purposes. Students must handle it with care.

B. Email:

Upon registration, an email account will be created for each new student.
Students are encouraged to use and check their USEK email account regularly. Important University information will be communicated to students through the email system.

The University does not allow students to update their email addresses with private or other email addresses. Only the assigned University email addresses will be used for communications with students.

Students are required to support the University’s efforts to ensure emails are secure and private, by not sharing emails passwords or other accounts with any other person. In fact there is no guarantee that the email address will remain private.

Email accounts are available to all USEK students and alumni.

Naming conventions of email accounts will be as follows:
FName.InitialFatherName.LName@net.usek.edu.lb

Using email safely:

Anytime you send or receive communications on the internet, there are opportunities for individuals to intercept your communication, in order to obtain your email address. IT services make every effort to ensure that the campus email service is secure. However there are some simple steps you can take to ‘play it safe’.

- Never open file attachments in email. Always save and check the file with a virus scanner.
- Never install software you receive via email unless you have checked it for viruses and spyware.

Unacceptable actions:

The following actions by a student are considered unacceptable:

- Use of USEK communications systems to set up personal businesses or send chain letters.
- Forwarding of USEK confidential messages to external locations.
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic or illegal.
- Introducing any form of computer virus or malware into the network.

Code of practice for all email users:

Students should adhere to the following guidelines for appropriate use:

1. Check your email regularly; once a day is an absolute minimum.

2. Beware of all email from unknown sources, especially those containing attachments. Delete such messages without opening them.

3. Personal use of the email system by students is permitted, but only within the scope of University policy.

C. Access to internet:

The primary purpose of internet availability in USEK is to provide access to information that will enhance and support the educational, instructional and research activities of students, Faculty and staff.

Faculty, staff and visitors can get access by logging in using their USEK username and password.

USEK users:

USEKwifi will be available at all locations in USEK. Students must connect to USEKWLAN then they will be automatically be given access based on the username they provide.

Features:

- Simple, secure wireless connection.
- Wireless connections available in every building on campus.
- Access to web sites is monitored and, in some cases, blocked.

Mobile devices (including Personal Digital assistant and cellular phones):

Mobile devices are portable, hand held devices that provide computing and information storage/retrieval capabilities for personal or academic use.

Developments in technology, and the business demands placed on users, have led to the introduction of many portable devices to access the University's resources, such as emails and internet.

Monitoring:

USEK acknowledges that internet use is a valuable business tool. However, misuse of this service can have a negative impact upon the University as a whole.

USEK reserves the right to block access to any internet resource and also monitors and records network traffic.

D. Hardware and software:

1. Do not tamper with the machines, reboot them, or shut them off for any reason. In addition, do not disconnect them from the network. If you encounter any problems while using the computer, please refer to the IT service desk immediately. This is the best way to prevent data loss or file corruption.

2. Students are not allowed to install software on lab machines.

3. Illegal copying of software is prohibited.

Personal computers and IT security:

1. As USEK is responsible for the information security of its own computers. The same rule applies to you.

2. Good information security practices require that up-to-date firewall and antivirus software are installed on your computer, automatic update of the operating system is enabled and security updates are carried out.

3. Be careful when carrying and storing a laptop. The laptop needs to be protected. Never leave your laptop in full view in your car.

Procedure in the event of any improper use of email or internet:

- The Director of IT services will notify a member of the SAO that a breach has occurred in the use of the University computer system.
- The SAO will consider the facts presented and, in case of inappropriate use, the Director of IT services will disable the user’s access until further notice.
- The academic registrar will be notified of the incident and will take the necessary steps (notify the student that his/her computer access has been denied).
- The SAO will carefully review the extent of any inappropriate usage, before dismissing the student.

Conclusion:

The IT Office has the operational responsibility for the University network and central computing resources. At the same time, it has an obligation to protect the confidentiality, integrity and availability of the network by ensuring that the resources are available and accessible.
In order to succeed in its task, the IT Office may monitor and respond to network breaches as they occur.

The University is committed to the provision of efficient and effective administrative support to serve the needs of the whole USEK community.