Information Technology User Policy

1. Introduction

1.1 USEK seeks to provide students and staff with reliable and secure access to the USEK local network, Internet and to an electronic messaging system via a network of personal computers (PCs).

1.2 This Policy applies to Faculty, staff and students as an independent document. Moreover the USEK Community is advised to abide by the University's Electronic Mail Etiquette when using email (cf. appendix 2). Users should be aware that the use of computing facilities is governed by legislation including:

- The Data Protection Acts
- The Copyright, Designs and Patents Acts
- The Computer Misuse Act

1.3 Any breach of these Acts will result in action being taken under the terms of the University's disciplinary policy and may be further escalated to law enforcement officers.

1.4 Staff and students with proper authorization may use the University internet and email facilities provided that they observe the Regulations and avoid the disruption of services for other users.

2. Policy

2.1 It is the University's policy to provide access to the internet and an email service for the use of staff and students, to facilitate reliable communications and to provide direct access to readily available sources of information for teaching, research, learning and University business needs.

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

2.3 Even though internet web site usage and email messages are not regularly monitored, the University reserves the right to intercept communications for inspection, should an incident occur where inappropriate use of the facilities is suspected. Any violation of the provisions (for example, downloading pornographic material, sending offensive messages, harassment, discrimination, spamming or hacking) may result in action up to and including dismissal under the University's Disciplinary Policy. In the event that legislative requirements are breached, the perpetrator(s) will also be subject to legal action.

2.4 It is important that all users understand and appreciate the values and dangers of using the Internet and email systems and follow the principles of the Policy and the terms of the associated Regulations and email Guidelines in order to safeguard their interests and those of the University. It should be noted that messages and data transmitted internally and to external sources are the property of the University and that all users have a responsibility to safeguard electronically accessed information against loss, disclosure or misuse.

2.5 In case of breaches of this Policy, the Regulations and in cases where there are irregularities, the perpetrators will be subject to University disciplinary processes and the law.

3. Internet Usage

3.1 Internet software may only be installed by or with the agreement of Director of IT Services. No unapproved or downloaded software may be used unless the integrity, continuity and full support of the product can be guaranteed. Software patches or updates may only be downloaded from officially supported vendors, subject to IT Services approval and ensuring strict adherence to the vendor's security and usage guidelines.

3.2 The University provides access to the Internet and its resources for the purposes of teaching, research and other University business. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out in the Policy and Regulations. Personal use must not interfere with the operation of University services, involve cost implications for the University or take precedence over the user's work accountabilities.

3.3 The University reserves the right to block access to any Internet resource. Academic access to blocked sites may be arranged on application via the Dean of faculty to the IT Services Department.

3.4 As indicated under section 2.3, Faculty and staff, must not access, retrieve, print or distribute text or graphical information that is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory, pornographic or otherwise obscene, defamatory or libelous, or any other material which contains illegal content prohibited by law or regulation.

3.5 Similarly, to protect University systems from imported viruses, the following operations are not permitted: downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet. Where such use is suggested for training or development purposes, it must have the specific agreement of the Dean of Faculty and Director of IT Services.

3.6 Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers, to deliberately release viruses or other harmful programs within either the University network or the internet or bypass security features.

4. Email Usage

4.1 Email accounts are available to all staff members, faculty members, students and alumni. Each staff and faculty member with an email account will be assigned a mailbox on USEK's mail server. However, students and alumni will be assigned a mailbox on Live@edu's mail server.

4.2 Naming conventions of email accounts will be as follows:

- Staff and faculty members' account name will be FNameLName@usek.edu.lb (i.e. Georges Charbel Eid: georgeseid@usek.edu.lb)

-Deans and Directors' account will be deanslist@usek.edu.lb

- Students' account name will be FName.InitialFatherName.LName@net.usek.edu.lb (i.e. Elie Pierre Khoury: elie.p.khoury@net.usek.edu.lb).

4.3 Email users should be aware that the boundaries between internal and external mail are now very blurred and it should not be assumed that email will remain within the University network.

4.4 Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory, pornographic or obscene, defamatory or libelous or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation or which brings the University into disrepute or which contravenes University policies. Information is understood to include text, images, sound and video; transmission is understood to include printing information and sending information via email. In particular, with respect to defamatory or libelous statements about another internal or external party, it should be noted that emails are discoverable documents in legal actions and may be used in evidence under the Regulation of Investigatory Powers.

4.5 All material contained on the email system belongs to the University Faculty and staff should not consider messages produced/received by them on University equipment/software (owned or licensed) to be secure. The confidentiality of email cannot be assured Faculty and staff should be aware of the possibilities of intended or accidental onward transmission to others beyond the original addressee(s). Furthermore, it is possible to retrieve deleted emails from back-up files intended to assure system integrity and reliability.

4.6 Security regarding access to the email system is of paramount importance as indicated in the Regulations. User identities and personal passwords must not be shared with others Faculty and staff should be wary of providing their email addresses to external parties especially mailing lists.

4.7 Faculty and staff transferring or receiving files or attachments from external sources should note that the University system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the IT Services Department immediately for inspection and action.

4.8 University email users are required to use this communication tool in a responsible fashion and to observe the related Regulations.

The University provides the email system for the purposes of conducting University business and it may not be used for personal gain or business activities unrelated to University operations. Faculty and staff must not use the system to promote an external cause or fundraising campaign without advance line management permission.

4.9 Reasonable personal use of the email system is permitted though subject to the approval of Deans of Faculty. They may define the level of use, as appropriate, in their areas. Personal use must not interfere with the operation of University services, involve cost implications for the University or take precedence over the user's job accountabilities.

4.10 Authorization to use the University PCs at home or University software on home PCs will be withdrawn on the termination of the employee's contract of employment. Then computer records of emails sent and received will be destroyed after a suitable period of time by the IT Services Department.

4.11 Where it is considered that there has been a breach in the use of the email system, any intercepted emails will be referred to the University Directorate for examination of the contents.

5. Responsibilities

5.1 The IT Services Department is responsible for the administration of those Policies and regulations concerning the use of University computer systems, networks and facilities. Overall accountability for Data Protection within the University rests with the Registrar, although operational responsibility for Faculty and staff data is held by the Head of Personnel and for student records is held by the Academic Registrar. However, all members of Senior Management, Directors of Departments and Deans of Faculties are responsible for the conduct and performance of their Faculty members, their usage of University facilities, equipment and their adherence to the contents of all Policies and Regulations.

5.2 Every University computer user agrees to abide by the terms and conditions set out in this Policy and the Regulations. Every user must accept responsibility for the protection of electronically accessed information against loss, disclosure or misuse.

5.3 All users must be aware of their responsibilities and obligations to others under the terms of the Data Protection legislation. Particular care must be exercised in respect of data held about other people both inside and outside the University for operational, research or any personal purposes.

Appendix 1

REGULATIONS FOR THE USE OF UNIVERSITY COMPUTER SYSTEMS, NETWORKS AND FACILITIES

(FACULTY, STAFF AND STUDENTS)

These regulations should be read in conjunction with University policies for the use of email, the Internet and other forms of electronic communication. Suspected misuse or abuse of University systems must be reported to the Director of IT Services or a senior IT Services representative in his absence.

Introduction

In general, members of the University may use those computing facilities provided that the use is related to their job (for Faculty and staff) or their course (for students). Modest use for private non-academic purposes is usually acceptable, however users must recognize that such exercise must not adversely affect the operation of the University. Faculty and staff should refer to the Internet and Email Policy on this and other related matters.
There are some activities that are expressly forbidden, because

1. They are illegal
2. They may disrupt services for others, and / or incur unnecessary cost for the University

The purpose of these regulations is therefore to protect the interests of users and to ensure that the University remains within the law. The University reserves the right to monitor network traffic activity and material held on the systems in order to ensure that users are complying with these regulations. User material or access to it may be removed if there are grounds for believing that it is in breach of the law or of these regulations.
In summary the regulations are:

- Users must comply with current legislation relating to the use of data networks, computers and computer-held information.
- Users must not attempt to gain access to systems or information for which they are not authorized
- If connection is made to links of external networks and facilities, the regulations governing the use of these facilities must be adhered to.
- Users must follow the University guidelines for maintaining security of systems
- Users must follow the University policies covering electronic communication
- Users must comply with practices to protect against computer viruses and other malicious acts
- Unauthorized copying and/or installation of software are strictly forbidden and will be reported to external authorities.

Penalties

Withdrawal of Facilities

Failure to adhere to these regulations may lead to withdrawal or restriction of access to University computing facilities, following discussion with the user's Dean of Faculty or Director of IT Department as appropriate.

Disciplinary Procedures

Any breach of regulations by Faculty and staff or students will be reported and dealt with under the University's disciplinary procedures.

Actions in breach of the law

All illegal action will be immediately reported to the Administration.

The Computer Misuse Act

It is an offence to access or try to access any computer system or material for which authorization has not been given. Any attempt to bypass security controls on a computing system is also an offence, as is facilitating unauthorized access i.e. the disclosure of a user id or password. The majority of University computers are networked, and it may be possible to connect to computers both within and external to the University, some of which may offer public services. However, being able to connect to a computer system does not necessarily mean that access to it is authorized.

The Copyright, Design and Patents Act

Almost all computer software in use in the University is protected under this Act, which gives the owners of the copyright the exclusive right to copy a protected work. It is therefore illegal to copy any software without the copyright owner's permission.

Software may only be used for the purposes defined in the licensing agreement, and on the computer systems to which that agreement applies. Terms and conditions of license agreements vary considerably from product to product. Further advice may be obtained from IT Services Department for any particular case.

Users must also ensure they have the permission of the copyright holder to publish material on web pages under their control.

The Data Protection Act

The Data Protection Act relates to the automatic processing of personal data and is applicable to computerized and also some manual systems. The Act gives individuals certain legal rights

regarding information held about them by others and sets requirements for organizations to meet before personal data can legally be processed.

Faculty and staff who process personal data must ensure that they comply with the Act and if in doubt must refer to the Administration. It should be noted that the automatic processing of personal data includes data that may be contained in email messages.

Authorized Use

All members of the University (students, Faculty and staff) will be registered to use the University computer facilities for the purposes of their academic studies or University employment. Upon registration or commencement of employment a computer account will be created and the new user issued with a unique username. All USEK network users will be required to sign acceptance of these regulations.

In some instances, visitors and conference delegates may apply through the designated coordinator for registration and access to the computer network whereby a small administrative fee is payable. IT Services reserves the right to refuse access.

Individually allocated user names are for the exclusive use of the person to whom they have been issued. This person is responsible and accountable for all activities carried out under their username. In particular, passwords must not be disclosed to any other person; good practice in the selection and use of passwords must be adhered to. Further details regarding such good practice may be obtained from IT Services Department, but in general:

- A password should be chosen carefully. It should not be a name or proper word and should preferably include some digits
- A password must be changed regularly (every three months is reasonable for most users)
- All users must identify themselves correctly at all times and must not attempt to withhold their identity or masquerade as another.

Use of external facilities
The University network provides access to other external networks and systems that have their own rules and regulations to which all users must adhere

Virus Protection
A virus is a program written to cause intentional damage to computer systems or networks, generally replicating itself from computer to computer across a network (downloaded from the internet or as an attachment to an email message).Moreover it can be perpetuated by the distribution of an "infected" external media device such as CD, DVD or USB flash memory. The degree of damage caused varies but many viruses destroy data and can significantly impair system operation. Virus scanning software has been installed on all networked PC systems on Campus.
However, all users must take the necessary steps to protect University systems from viruses by adhering to the following rules:

- Any software programs must not be installed or executed without the prior approval of IT Services such as:
- Computer Games
- Public domain software, shareware or peer to peer software
- Any unauthorized program attached to an email message
- Any programs obtained from the Internet

The following categories of computer media must always be scanned for viruses:

- Any item originating from outside the University
- Any item used on a home computer removable storage devices such as CDs, DVDs or USB flash memories
- Computer magazine cover disks
- Free mailings

Unacceptable Use of University IT facilities

In addition to the above, the following are specifically defined as unacceptable usage of University computers and networks (this list is not necessarily exhaustive).

University systems and networks must not be used for:

- The sending of messages which are racially, sexually or personally abusive
- The corruption or destruction of other users data
- The initiation or spread of electronic chain mail or SPAM
- Any activity which is wasteful of resources such as playing of computer games
- Defamation or libelous attacks on persons
- Any activity which may reflect adversely upon the University

Behavior in IT Classrooms or Labs

- It is suggested that no food or drink should be consumed in computer laboratories, as those responsible for any spillage resulting in damage to equipment will be held accountable for the cost of repairs.
- Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities.
- No equipment should be moved from its designated place or be tampered with in any way such as changing workstation characteristics.
- Users should not act in a way so as to deliberately or recklessly overload access links or switching equipment.
- Printer stationery should be used for the purpose for which it is supplied. The theft of printer paper will be dealt with seriously.

Disclaimers

The University takes no responsibility for the malfunctioning of any equipment or software, the failure in security or integrity of any stored program, data, email content or Internet download. No claim shall be made against USEK, its employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

USEK will not be liable for the content of email messages or any attachments therein and the text of said emails does not reflect the views of USEK, Faculty or staff.

Appendix 2

EMAIL ETIQUETTE

(FACULTTY, STAFF AND STUDENTS)

1. Introduction

Even though Electronic mail is one of the primary means of communication its quickness and easy conventions render it under developed. Although email is more flexible and in some ways easier to use than a traditional format, it has its own limitations and can still be used as evidence of a wrongdoing.

The following sets down some points of good practice for both senders and receivers of email in order to effectively use this medium.

2. Some characteristics of email

In considering the use of email, it is worth noting some of the following characteristics:

Email cannot be regarded as private or secure. Avoid sending confidential information via email unless an encryption tool is available.

- Messages cannot be totally erased: even when deleted they can be retrieved from backups and usually traced back to their origin.
- Messages can be stored since unlike telephone conversations, they are not ephemeral.
- Messages can be printed therefore cannot be regarded as purely electronic.
- Messages can be readily sent to a large number of recipients and forwarded many times.
- Forwarded messages can be invisibly edited (unlike a memo which is fairly obvious if it has been altered).

Depending on the way in which it was sent, recipients who are on a distribution list may be unaware that they are not the only ones to receive the message. They may also not know who the other receivers are.

3. Sending Email

- Is email really the most appropriate medium?
  If you are composing a message that is long or requires some care in its construction, ask yourself whether a letter or memo might be more appropriate.
- Messages should be short and to the point in order to be most effective.
- Do not send emails without subjects.
- Clearly identify the topic in the subject field.

- A message should be about a single topic. If you want to raise a second topic, send another message to avoid having content unrelated to the message heading.
- If you need to cover several related topics, try to make the subject label broad enough to cover the whole issue. Multiple topics are confusing and frustrating for someone trying to follow a thread through email correspondence.
- You can never be sure what system your recipients will use to view your message. Even though email systems like Outlook encourage you to format your messages, it may not survive for your recipient. Therefore, treat all messages as plain text (avoid using £ signs - use GBP instead).
- Use appropriate spelling, grammar and punctuation. Always proof read and use the spell checker if necessary. Messages are frequently printed so the errors that may be overlooked or excused when read on screen are likely to be judged more harshly when seen on paper.
- Choose words carefully since hastily produced messages can be misinterpreted.
- Avoid slang.
- Do not include anything that you would have reservations about appearing in print above your signature.
- Be careful of your 'tone of voice'. Because your facial expressions and verbal tone are missing from electronic correspondence, your text is open to misinterpretation.
- Avoid sarcasm or other forms of dry humor to minimize the risk of misinterpretation.
- DO NOT USE ALL CAPITALS, AS IT MAY BE INTERPRETED AS SHOUTING!
- You should make it clear if you do not wish your message to be forwarded by its first recipients.
- Think carefully before sending confidential information about yourself or others. If your message refers to a colleague or their work make sure you include that colleague in the circulation of the message.

4. Replying to Email

- If possible reply within 24 hours. If you cannot answer a message within this time, send a message stating when you will be able to respond.
- Consider using 'Sabbatical' when on leave or out of the office for any period of time making sure you give a contact name for urgent messages. However, remember that if you are on a mailing list it can be irritating to receive "Out of Office" messages from unknown individuals
- Change the subject line if the topic changes in your reply.
- Use a signature that gives contact information i.e. extension number and department.
- Do not include the original message automatically. Consider whether it is necessary or not.
- Try to formulate your reply intelligibly on its own without referencing back to the original message.
- When responding to a message sent to several colleagues, check whether anyone else has already responded.
- When responding to a message that has been sent to a list of recipients, only reply to the whole list if your answer is of interest to them all! If you are taking up specific points with the sender of the original message, send your response only to that person.

- Watch ccs when replying to make sure you reach your intended audience and to reduce the volume of unnecessary material sent to others.

5. Forwarding Email

- Watch out while forwarding a message: would the original sender wish you to do so? You may need to seek their permission first.
- It may be a good idea to remove a lengthy distribution list from the head of a message before forwarding it. A note indicating our intentions would be appropriate when a change is made such as this.
- If you edit a message before forwarding it, make sure your recipient knows that.
- Reduce the amount of unnecessary material included in a forwarded e-mail.

6. Email Addresses

- Where there is more than one user with similar names, double check that you have chosen the right one.
- The same rule applies to Users' internal email addresses.
- Keep any personal distribution lists up to date.

7. Email Attachments and Filing Email

- Limit sending large files so that the e-mail Server system does not risk being impaired.
- Instead of sending a message with an attachment to a large distribution list, place it in a shared area and email people with the filename and its location or onto the University intranet.
- The mail server supporting the email system is not intended for the long-term storage of messages. When you receive an email message with an attachment, save the attachment in a designated drive.
- Housekeeping of stored messages is your responsibility. From time to time you should go through your stored messages deleting those that are no longer needed.

8. Unwanted Email

- You can limit who gets hold of your email address by being circumspect when visiting web sites and by thinking carefully before subscribing to any mail service.
- Do not reply to 'junk' e-mail blocking the way to any sender who thinks that your e-mail is “live”.
- The best way to deal with 'junk' e-mail is to delete it.

9. Think Before You Send

- Email is an effective way of communicating but if handled improperly, the benefits will be lost. Please be aware that email communications can be presented as evidence in the court of law and are legally binding.

Appendix 3

PROCEDURE IN THE EVENT OF ANY IMPROPER USE OF EMAIL OR THE INTERNET

When there is a breach in the use of the University email / Internet system, the following Disciplinary Procedures will be put into practice.

FACULTY AND STAFF

- The Director of IT Services will notify a member of the SAO that a breach occurred in the use of the University computer system.
- The SAO will consider the facts presented and if it was proven that there has been inappropriate use, the Director of IT Services will disable the user's access until further notice.
- The user's superior will be notified of the incident by the Head of Personnel.
- The user will be notified by the Head of Personnel that their computer access has been denied pending an inquiry into the inappropriate use of the University computer system.
- The SAO will review carefully the extent of any inappropriate usage before taking any steps further.
- In those circumstances where a member of Academic staff is alleged to be in breach of the Code of Practice, such allegations will be investigated by the Registrar, the Head of Personnel and the Director of IT Services. The results of the investigation will be reported to the Rector who will ultimately decide if the University Disciplinary Procedure should be invoked.

STUDENTS

- The Director of IT Services will notify a member of the SAO that a breach occurred in the use of the University computer system.
- The SAO will consider the facts presented and if it was proven that there has been 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 be asked to write to the student advising that their computer access has been denied.
- The SAO will carefully review the extent of any inappropriate usage before dismissing the student.