

# UCSI University

## ICT Policy Manual

---

Version 1.3

---

Date: Dec 2009

---

## TABLE OF CONTENTS

1.0 Introduction	6
2.0 Acceptable Use Policy	7
3.0 Electronic Mail Policy	8
4.0 Anti-Virus & Anti-Spamming Policy	9
5.0 User Password Policy	10
6.0 Data Backup & Restoration Policy	11
7.0 Mass Email Policy	12
8.0 Procedures, Guidelines & Standards	13

## 1.0 INTRODUCTION

Information and Communication Technology (ICT) resources at the UCSI University(UCSI) are intended primarily to serve the teaching, research and administrative purposes of the University. The University is therefore responsible for ensuring that resources and facilities it has provided are in fact used for the purposes for which they were intended.

The University grants members of the University community shared access to these resources in support of accomplishing its vision and mission. Access to University ICT facilities and resources is a privilege and not a right. This privilege is extended to all faculty, staff and students and may be limited or revoked if the user violates University policies or guidelines. All users of these ICT resources are therefore required to use them in an effective, efficient, and responsible manner.

The ICT Policy Manual contains the following policies, procedures, guidelines and standards:

- A. Acceptable Use Policy
- B. Electronic Mail Policy
- C. Anti-virus and Anti-Spam Policy
- D. User Password Policy
- E. Data Backup & Restoration Policy
- F. Mass Email Policy
- G. Procedures, Guidelines & Standards

## 2.0 ACCEPTABLE USE POLICY

### PURPOSE

The purpose of this policy is to ensure the proper use of UCSI's ICT facilities, software, services and systems (hereinafter collectively known as ICT resources) by its employees (academic and non-academic), guests and students (hereinafter collectively they are known as the community) in an appropriate, responsible, and ethical manner. This policy also applies to the use of privately owned computers or notebooks connected to the University network.

### USERS' RESPONSIBILITY OF UCSI'S ICT RESOURCES

The community as a whole must be warned that they must not use the facilities, software, services and systems in any illegal or otherwise unauthorized manner.

UCSI reserved the rights to monitor and record all activities within the university when the community access the facilities, software, services and systems.

Any violation of this policy and/or procedure will be dealt with accordingly by the rules, regulations of the University and disciplinary actions will be taken.

Users who violate this policy may be denied access to university ICT resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Violations will normally be handled through the university disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Student Affairs. However, the university may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing ICT resources or to protect the university from liability.

## 3.0 ELECTRONIC MAIL POLICY

### PURPOSE

The purpose of this policy is to ensure the proper use of UCSI's electronic communication infrastructure system by its employees (academic and non-academic), guests and students.

### INTRODUCTION

As an institution to promote, create, acquire, share and disseminate knowledge, UCSI University provides for members of the UCSI community an electronic communication infrastructure that includes computing resources, network connectivity, and software tools for electronic communication (e-mail). This infrastructure is the property of UCSI and is provided for the purpose of supporting academic (teaching and learning), research, administrative functions of the college, business communication and other creative endeavours. With this provision, UCSI strongly encourages the free exchange of ideas and information within its community and members of other communities throughout the world.

The community is reminded that use of e-mail is a privilege, not a right and should be treated as such by all users. The users have the responsibilities to use this resource in an efficient, effective, ethical and lawful manner at all time. Employees are permitted to use e-mail in a prudent manner for personal communications as long as such personal use does not interfere with the employee's performance of his or her job responsibilities or the business use of the e-mail by other employees.

UCSI is committed to providing an educational and work climate that is conducive to the academic and development of each individual. UCSI protects the rights and privileges of every individual and also enhances self-esteem of its community. The community should be aware that any form of harassment or discrimination against any individual is inconsistent with the values and ideals of UCSI community and is not permitted within the context of the electronic communication infrastructure.

UCSI makes every effort to observe the confidentiality and privacy of software, files, and materials stored and or transmitted by UCSI computer equipment. Since confidentiality and privacy is not readily attainable when using e-mail, employees should never use e-mail to send any message that would be a source of embarrassment to the sender, to the recipient, or to UCSI if the message were to be seen and receive by others.

In providing and maintaining its electronic communication infrastructure, UCSI as much as possible complies with existing federal, local laws and Cyberlaws of Malaysia; and it requires that the community do the same. UCSI also enforces its own policies, rules and standards pertaining to the electronic communication environment.

## SCOPE

All e-mail communications (and associated attachments, objects, graphics, videos) transmitted or received by UCSI network are subject to the provision of this policy, regardless of whether the communication was sent or received on a private or UCSI owned computers. When faced with evidence of violations of the UCSI policies or standards, of contractual obligations, or of federal, local or Cyberlaws of Malaysia, UCSI may consider the e-mail communication and its associated stored on or transmitted by UCSI computer equipment to be property of UCSI and may inspect them without notice.

## E-MAIL RESPONSIBILITIES, PRIVACY & CONFIDENTIALITY

E-mail is a privilege and should be used responsibly. Individual users using the UCSI's computer facilities must assume full responsibility for their acts. UCSI cannot and will not attempt to protect individuals from material that may be offensive to them, except in cases of violation of the laws of the country, UCSI policy and standards, and in these cases only where technically feasible. Individuals making use of electronic communications are warned that they may willingly or unwillingly receive or discover electronic or hardcopy material they find offensive. UCSI will not establish additional standards, beyond those that are already legally relevant. UCSI assumes no responsibility for the initiation or transmission of such material, whether or not such material originates inside or outside the UCSI.

Most e-mail users may intend their message to be private communications between themselves and another party, the privacy and confidentiality of e-mail cannot be guaranteed by UCSI for many reasons. For example:

- E-mail messages may be saved indefinitely on the receiving computer.
- Copies of e-mails can be forwarded electronically or printed on paper.
- E-mails can be intentionally or accidentally forwarded to others.
- E-mail messages may be sent to incorrect e-mail addresses or be improperly delivered by an e-mail system or Internet Service Provider (ISP).

- It may be impossible to find out who sent a message, especially if it is passed on by many people.
- It may be possible for other people to read or change messages that you send by forwarding it to others.

Although employees are permitted to use e-mail for business, private and confidential communications, they should be aware that there are more appropriate ways of communication available for matters requiring privacy or confidentiality.

Individuals must assume full responsibility and accountability for their actions. UCSI offers a powerful tool for communication, but there are potential risks that come with it like the infringement on the rights of others. Individuals should consider carefully how their actions affect other users of the community, and whether their behaviour is against the UCSI policy and standards, or federal law, local law and Cyber laws of Malaysia. A policy or guide usually cannot act as a substitute for common sense in handling certain situations.

UCSI reserves the right to examine material stored on or transmitted through its communication infrastructure. UCSI will examine files only when, and to the extent that, reasonable business needs require official intervention for the protection and maintenance of the communication infrastructure. The community of UCSI should be aware that privacy cannot be guaranteed in electronic communications, even for information or communication that has been deleted.

## CODE OF BEHAVIOR

There are situations and matters not controlled and covered by any law or policy, UCSI expect members of its community to exhibit acceptable ethical conduct in the use of computing resources. Electronic communication can be ambiguous and is less personal in nature as compared to other tools and form of interaction. Individuals are expected to exercise good judgment to ensure that their electronic communications reflect the high ethical standards of the academic community and display mutual respect. While UCSI will not restrict access to or filter any form of information, individual using computer workstations or displays in public areas or labs are encouraged to maintain an appropriate level of common civility and courtesy in viewing information content that could be identified as offensive or causing embarrassment to a passer-by or casual observer.

UCSI expects members of its community to know and familiarize themselves with copyright laws with regards to the educational environment and to understand the nature of the special privileges ( known as "fair use") extended by most laws to lecturers and students in the limited reproduction of copyrighted materials for their personal use. The provision of "fair use" by these laws must be

kept within legal limits in their use of copyrighted materials in the electronic environment. Posting any copyrighted material in an electronic form that is accessible by others within and outside of the community, even if for the purpose of personal use, is in violation of law and is prohibited. Similar prohibitions apply to the posting of registered trademarks, brand name, or protected symbols or graphics and the use/or distribution of computer software or other electronic information and published material without permission or consent of the copyright owner.

## MONITORING OF ELECTRONIC COMMUNICATION (E-mail)

Responsibility for the electronic communications infrastructure is delegated to the Deputy Vice Chancellor, who assigns authority to the Computer Services Department for its day-to-day management. Deputy Vice-Chancellor does not intend to monitor e-mail usage by its users in a regular or systematic manner; however, it does reserve the right to monitor such usage from time to time and without prior notice. Such monitoring may include tracking addresses of e-mail sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages. E-mail monitoring which focuses on a specific individual or a selected group of individuals, must be based on a reasonable suspicion of misuse or wrongdoing and must be approved in advance by the Vice President of Administration may take corrective action or disciplinary action against the user based upon the information obtained from monitoring or inspecting his or her e-mail communications. Furthermore, Deputy Vice-Chancellor may disclose e-mail communications sent to, receive by, or relating to a user to law enforcement officials without giving prior notice to the user.

## E-MAIL ACCOUNTS

Each user is given an e-mail account with prior login and password to access into the network. Passwords should not be given to other people should be kept confidential and be changed frequently. Passwords must not be written down, or used in any other processes that facilitate automatic log-on. The mailbox owners are responsible and are liable for all messages sent from their e-mail accounts. E-mail accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account name or password with another person. Account owners are ultimately responsible for all activity performed under their account. The only exceptions to the above are secretarial functions that have responsibilities for their managers' e-mail.

## DISCLAIMER AND CONFIDENTIALITY NOTICES

E-mail has many hidden dangers especially when it is use for external electronic communication and sent outside of UCSI. E-mail messages can be used as evidence in a court of law if required. It is good practice to insert the following message into all external e-mails:

- a) Electronic communications via the Internet are not secure and therefore UCSI does not accept legal responsibility for the content of this message. Any views or opinions presented are solely those of the author and do not necessarily represent those of UCSI.

Or

- b) This e-mail and any attachments transmitted with it are private and confidential to the named recipients. Any information provided is given in good faith. It may not be disclosed to or used by anyone other than the recipient (s), nor copied in any way. UCSI accepts no liability for the content of this e-mail, or for the consequences of any actions taken on the basis of the information provided, unless that information is subsequently confirmed in writing. If you have received this e-mail in error, please advise the sender, and then delete it from your system.

## PERSONAL USE (EMPLOYEE ONLY)

The main purpose for providing e-mail at UCSI is for official business activities and not personal use. Responsible personal use is permitted, provided that it is reasonable and:

- Is not likely to cause UCSI loss
- Is not for personal gain
- Does not contravene any of UCSI's policies and guidelines.
- Is not detrimental to the UCSI's image
- Does not interfere with work

If user is unsure about the material they wish to send, or are concerned about any material, which they may have received, they must discuss this with their immediate supervisor. Users are prohibited from engaging in any of the practices described under the section "PROHIBITED E-MAIL PRACTICES" and if found doing so are subject to normal Human Resource disciplinary actions.

## LEAVERS (EMPLOYEE ONLY)

Once an employee resigns or leaves and upon notification from Human Resource and/or users' immediate supervisor, a leaver's e-mail account will be deactivated with immediate effect. Any incoming e-mail will be allowed for 5 following days and will be printed on hardcopy for the user if requested.

## MANAGING E-MAIL ACCOUNT & DOCUMENT

Just because the communication is electronic there is no reason not to apply good technique to the management of the e-mail. The more you use e-mail, the more important it is that you manage it and therefore your time effectively. There are certain activities that users should carry out regularly on the e-mail system. How often you perform them will not necessarily be the same for all activities and may be influenced by the nature of your work.

1. Read all the new e-mail messages at least once in every 1 or 2 days
2. Do not let messages build up in your Inbox.
3. Reply messages as soon as you can.
4. Delete messages as soon as you no longer need them because a fixed amount of storage space is available for each user.
5. New e-mail will be prevented from coming in to the mailbox once the mailbox has reached the maximum allowable storage space.
6. Any messages, which users want to keep, should be saved onto the hard disk or floppy disk.
7. Open your 'Sent messages' folder at least once a week and delete old messages that you no longer need.
8. Set an auto-reply when you are likely to be out of the office for some time.
9. The nature of your work may require you to retain a hard copy of the e-mail message, it is necessary you print the e-mail and store the hard copy in the relevant subject matter file as you would any other hard copy communication.

## PROHIBITED E-MAIL PRACTICES

Members of the community are prohibited from engaging in any of the practices described below on UCSI electronic communication infrastructure. UCSI through the Computer Services Department may suspend or revoke the e-mail privileges of any individual who abuse them. In addition to that, UCSI may impose appropriate sanctions, ranging from reprimand to suspension or termination, upon an individual who engages in one or more of the following activities:

1. Sending obscene, offensive or causing embarrassment e-mail (or attachment) without the consent of the recipient;
2. Sending intimidating, threatening, harassing or abusive e-mail (or attachment) to another user;
3. Intercepting, disrupting, or altering an e-mail message (or attachment) without proper authorization;
4. Attempts to read, delete, copy or modify e-mail (or attachment) of other users without permission;
5. Messages should not be read or sent from another user's account except under proper delegate arrangements;
6. Forgery (or attempted forgery) by misrepresenting the identity of the source of an e-mail message;
7. Allowing another user (known or unknown to UCSI) to use one's e-mail account for fraudulent purposes;
8. Using e-mail to interfere with the ability of the others to conduct UCSI business
9. Sending unsolicited junk e-mail, "for profit" messages, or mass electronic mails without a legitimate UCSI business purpose; Please refer to a separate policy known as "Spam Policy"
10. Using electronic communications infrastructure (accessing web based e-mails and search engines) for commercial purposes unrelated to UCSI business;
11. Reproducing or distributing copyrighted materials without appropriate authorization;
12. Unauthorized exchange or selling of propriety information, trade secrets or any privileged, confidential or sensitive information that belongs to UCSI;
13. Registration to list servers without proper authorization from your supervisor, such service subscription can result in an overload of received messages directly impacting the performance of the e-mail system;
14. Users cannot compromise the privacy of their password by giving it to others or exposing it to public view;
15. Using electronic communications infrastructure for any purpose, which violates federal, local and Cyber law of Malaysia as well as UCSI policy.

The above list is just an illustration and by no means exhaustive.

## STANDARDS

E-mail is a business tool and all users should treat it like you would any other business tool such as telephone or facsimile. E-mail offers a fast, easy and flexible way of communicating as well as an effective mode of sharing information. Because e-mail is easy to use and flexible, the risks

associated with it are often overlooked. It is not free, it is not confidential and, like any computer system, it is not totally reliable, UCSI would like to remind all users to remember and adhere to the following standards when using e-mail systems.

1. Do not send an e-mail to someone to whom you would not send a letter.
2. Do not write something in an e-mail that you would not write in a letter or say to someone's face.
3. Do not send an e-mail to someone by using another user's e-mail account.
4. Only send message to people who need to receive them - do not copy them unnecessarily.
5. E-mail messages must not contain material which is illegal or which could offend or harm anyone. If you (employee) receive a message, which contains this type of material, tell your supervisor as soon as possible and keep it as evidence. You must not pass it on to anyone else. For student, please see your Counsellor or Head of School.
6. Do not use e-mail to enter into a contact, or change or end an existing contract with and organization
7. Keep your password confidential.
8. Any secret or restricted information you send by e-mail must be protected. One way is to by putting the information in an attachment (such as Microsoft Word or Excel file) and protecting the file with password. Use another method (such as telephone) to give the password to the person you want to receive the information.
9. Do not rely on the e-mail system to store message over a long period of time. If you want to keep messages for a long time, you should save them in a file storage system.
10. E-mail can be used as evidence in a court of law. Therefore you should consider how long you need to keep your messages. If your messages are to do (potential) with legal disputers, you should print them and keep the hardcopy in a safe place.
11. Use software to detect viruses on your workstation or computer so that when you open an attachment, it is automatically scanned for viruses. Typically, if you receive an attachment from an unknown sender, do not open it unless you can confirm it is from a reliable source. You have a choice to delete it or reply the e-mail and request the sender identity to be made known to you.
12. If you workstation or computer is logged into an e-mail system and you leave it unattended, you should switch on your password protected screen saver if you have one. If you won't try to save the e-mail messages offline in another file and logged off.
13. Be careful what you write. E-mail is not the same as conversation. It is a written record and can be duplicated freely.
14. Use normal capitalization and punctuation. For business and official purposes, e-mail message should not contain emoticon or smiley.
15. Reply soon to messages, especially if UCSI customers or students send them.
16. E-mail messages should have a structure just like a letter especially for official purposes.

17. Check the spelling.
18. Do not use attachment unnecessarily. Attachment to e-mails can increase the size of the information that is sent over the networks. This can cause the networks less efficient.
19. Do not keep attachments in the e-mail system. Save them with your other files. Also, do not leave messages in the e-mail system just because you want to keep the attachments.
20. Do no spam and please refer to a separate policy for spamming.

The above list is just an illustration and by no means exhaustive. Some of the standards may be quite subjective and could be found to be highly debatable by users. If you have been practicing good and better e-mail standards than those listed above, please continue to do so. If you short of some of the above good practices, treat this as a reminder for improvement.

## AMENDMENT

Members of the community are required to comply with UCSI's Electronic Mail Policy. UCSI reserves the right at its discretion to amend, suspend or withdraw any section or part of this policy or any related policy by way of general notice, to take immediate effect. This policy is always available in the Computer Services Department, posted in the local Intranet-based document, Human Resources Department, Counselling Centre, Schools and Library. It is the responsibility of the user to review this policy from time to time.

All amendments in the future will be accompanied by a date on the first page of the policy with an appropriate version number. It is recommended that user access the local intranet regularly to review this policy for changes.

## ANNOUNCEMENT

- a) Their respective Schools will inform new students about this policy during the orientation week.
- b) Individual who provide them the access prior to using the e-mail facility must inform guests about this policy.

## 4.0 ANTI-VIRUS & ANTI-SPAMMING POLICY

### PURPOSE

The purpose of this policy is to ensure that the University will provide its community adequate protection from computer virus, unsolicited and unwanted emails from internal or external sources by investing and deploying anti-virus and anti-spamming software where appropriate on ICT facilities owned or leased by the University and ICT services provided by the University.

### IMPLEMENTING ANTI-VIRUS & ANTI-SPAMMING PROTECTION

With the introduction of these policies, the University

- a) ensures its community is protected from virus, spy ware, malicious attacks, phishing and not inconvenienced through the receipt of unsolicited emails.
- b) ensures its community do not use the ICT resources in the manner that is illegal against others
- c) seeks to minimize any misuse or illegal use of email communications

The University will install anti-virus software to ensure that all networked computer servers, computers and notebooks owned by the University are protected against virus infection. The effectiveness of these policies within the community is dependent on individual due to the uniqueness of the personalisation feature and usage. This is due to the fact that anti-virus and anti-spam software can be turn OFF and ON by the individual user and filter options can be adjusted. However, it is expected that the number of spam emails and virus attacks be reduced.

These software(s) are updated on regular basis.

## 5.0 USER PASSWORD POLICY

### PURPOSE

The purpose of this policy is to ensure the user has the minimum standard applied to their user password to support the confidentiality, integrity and security of the University ICT resources. The objectives are to ensure access control to the ICT resources, to communicate the needs to have protection against unauthorized access and to establish an ICT environment that will encourage data sharing and exchange without sacrificing security.

### USER RESPONSIBILITIES

All users have the following responsibilities:

- a) All user passwords are to be seriously treated as private and confidential and must not be divulging, shown or given to any party other than the user.
- b) User passwords must be change on regular basis or at least every six months.
- c) It is recommended to create a password based on combinations of numeric and alphabetic with a minimum length of 8 characters.
- d) It is not recommended to have password that is the same as the username, recycled or previous passwords or name which is associated with the user (i.e. DOB, company name or horoscope etc.)

Users issued with a username and password for the first time has the responsibility to change the password immediately after he/she has been issued the initial default password.

Users must not share the password with others and must not write or keep the password in an insecure location. Password must be protected and kept in a secure place.

Note: A Username is a name used to identify an account and associated to a password.

## 6.0 DATA BACKUP & RESTORATION POLICY

### PURPOSE

The purpose of this policy is to define the backup and restoration of data and information associated with the University operations. This policy applies to only staff of the University who create, process and store data and information using the ICT resources. With this policy in place, we can ensure copies of critical data are retained and available in case of disaster, software or hardware failures.

### BACKUP OF CRITICAL DATA AND INFORMATION

The Computer Services Department is responsible to backup the entire critical corporate database for the entire University which is located at the servers. Individual users and staff will be responsible to backup their own data which is on their own desktop and notebook computers. The University provides the necessary storage and backup media to staff who request for it in order for them to perform the backup process.

The corporate database is backup on disk media and it is kept in a different location which away from the servers. The backup disks are periodically tested to ensure they are recoverable. All backup disks are clearly marked for ease of identification with name and creation date. The current policy is to backup the corporate database on a daily basis after office hours. All the backup disks are kept in an offsite locked placed only known to Head, Computer Services Department.

## 7.0 MASS EMAIL POLICY

### PURPOSE

The purpose of this policy is to define the Mass Email which is to be sent out electronically to a large, selected group of the University users. This policy will specify the details and standard to which the format, content and authorization needed for sending mass email.

### SENDING MASS EMAILS

All email sent in the form of Mass email must receive prior approval from the VP of Corporate Communications or Head of Human Resources or Head of Computer Services Department. The list of member email addresses that are to receive the email (or recipient list) must get prior approval from one of them.

Sending Mass Emails to the recipient list is the responsibility of the Computer Services, Corporate Communications or Human Resources Department. Just like any normal emails, Mass email requires the following information:

- Who is the email message intended to? all staff, student or group
- What is the subject?
- Who is the email message from? i.e. email address
- What email address to reply to? This may be different from the email address of the sender.

The content of the mass email is the responsibility of the original user who created the message and the Authorizing person. Messages must be electronically signed with the name, position and contact information. If the message is lengthy, it is recommended to provide additional URL links to the email. If possible the text message should be limited to just one page or less.

## 8.0 PROCEDURES, GUIDELINES & STANDARDS

### USE OF SOFTWARE ON THE COMPUTERS & NOTEBOOKS

University administrators (Deans, Directors, Head of Department and Managers) must be proactive in managing and monitoring the computing software used on the computers and notebooks in their departments or schools. Mismanagement of this ICT resource may bring a considerable liability to the University. Copying protected software also conflicts with the fundamental values of the University community regarding intellectual property.

Specific steps that can be taken to ensure against copyright infringements on software include:

- a) Identify the person who will be responsible for software on account or departmental machines.
- b) Encourage staff to purchase computer software through the Purchasing Department.
- c) For software distributed through Purchasing Dept., retain the documents as evidence of purchase for each piece of software.
- d) Encourage staff to request the assistance of Computer Services Dept. to install any software on computers or notebooks.
- e) Where staff installs copies of personally owned software on University machines, regardless of how the software was distributed, require them to identify such software for departmental inventory, and encourage them to provide a copy of the purchasing documentation for the departmental records.
- f) For software obtained through shareware distribution mechanisms, retain and file specific evidence of payment made for each piece. (Such shareware usually specifies that if the package is being used in a commercial environment, a license fee must be paid. The University is considered a commercial environment, making it likely that the fee is required.)

### USE OF INTERNET BANDWIDTH WITHIN THE CAMPUS

The University is committed to pursuing an efficient and fair network usage in order to meet the growing bandwidth requirements of the entire University. The aim of this section is to manage bandwidth use to avoid degradation and ensure network efficacy. Management of Bandwidth resources shall be entrusted to the Computer Services Department. Bandwidth usage shall be subject to the following:

- a) Internet Bandwidth will not be over utilized as to prevent access to critical information, research and online educational material. Bandwidth allocation shall be made in the following order:
  - i. UCSI applications and portal
  - ii. e-mail
  - iii. internet research
- b) Unauthorized persons/users are not allowed to access internet facilities within the campus network
- c) ICT resources shall be monitored from time to time by the Computer Services Department for efficiency and optimal usage by all the users.

The University will consider urging all users to be considerate when using the internet services so as not to cause unnecessary download of materials or upload of materials through the internet which may clogged the internet line which may be used for more important and critical information and applications.

## USE OF COMPUTING LAB & GUIDELINES

Students are to adhere to the following guidelines while using the computing labs:

- Do not bring food or drink into the computer lab.
- Smoking is not allowed in the computer lab.
- Report problems promptly to Computer Services Department.
- Do not alter the configuration of hardware or software. This has been set up to cater for a wide range of users.
- Leave each piece of equipment set up as you found it. Do not remove any items from the computer lab.
- Follow any directions posted in the venue by Computer Services Dept. staff.
- Labs are available for use only by University staff and students and authorised external users.
- Unofficial work of a personal, non-profit nature is permitted, provided official work is not affected.
- Non-University related commercial activities are not allowed.
- Do not waste computer resources (e.g. unnecessary printing) or disadvantage other users by monopolising equipment, network traffic, etc.
- Keep the computer lab clean and free of hazards.
- Do not place software or other files on University computers where these may lead to damage or legal charges (destructive programs such as viruses, pirated software, etc.).

- Do not use the facilities to make unauthorised copies of copyright, licensed or patented material.
- Do not use the facilities to defraud or to create false or misleading information.
- Do not act as though you intend to break the law. Do not attempt to guess an access key or password to gain unauthorised access to local or remote computers.
- Do not attempt to access any areas of any systems for which authority has not been granted.
- Do not attempt to monitor or read another user's files or communications.
- Report unethical activity to University staff promptly.

## STANDARD OPERATING ENVIRONMENT FOR SOFTWARE AND COMPUTERS

Due to the variety and nature of work performed by staff and students across the entire university, it is not practical and easy to define a standard operating environment for all areas and users. It is however, in the desire of this section to provide details of the standards with the intention of encouraging consistency wherever possible and practical. The University is also aware of the individual needs of the School and Department but at the same time stress the importance of compliance with as many components of the standards as is practical in the short term, with a longer term view of meeting the full compliance in order to have good support from the Computer Services Department and reduce the cost of ownership.

The recommended standard software installed on all new computers:

STANDARD	OPTIONAL	
Microsoft Windows XP, Vista or 7	Microsoft Visual Basic 6.0	Microsoft Project 2003
Microsoft Office 2003 and 2007	Microsoft Visual Studio 2003	Microsoft Visio 2003
Internet Explorer 8	Microsoft Visual Studio 2005	Microsoft FrontPage 2003
Kaspersky Anti-virus	Microsoft SQL Server 2000	Nero 7
Adobe Reader 9	Microsoft SQL Server 2005	Matlab
Microsoft Outlook	Crystal Reports 9	
Any other softwares that come with the computer.	Crystal Reports 11	
	Oracle 10g	
	Macromedia MX 2004	

The minimum standard applies to only new purchased computers for laboratory and staff as well as notebook for staff:

ITEMS	DESKTOP COMPUTER	NOTEBOOK COMPUTER
Processor Speed :	Intel Core2Duo 2.5 GHz and above	Intel Core2Duo 1.8 GHz and above
Memory :	2GB DDR2 667MHz RAM	2GB RAM
Hard disk :	120GB Hard disk	120GB Hard disk
Disc Drive :	DVD-ROM / DVD-RW	DVD-RW
Monitor :	Samsung 17" LCD Monitor	Built-in
Display :	17" or 19"	14.1" Widescreen
Network Interface Card :	Yes	Yes
Modem :	Yes	Yes
Sound Card :	Yes	Yes
Graphic Card :	Yes	Yes
Wireless Card :	Yes	Yes
Bluetooth :	---	Yes
:		
:		
:		