KING CEASOR UNIVERSITY

ICT POLICY

1. INTRODUCTION

1.1. King Ceasor University("KCU") offers a wide array of computing and networking resources and services to its stakeholders (students, staff and partners). These services are in place to facilitate teaching and learning, research, and administrative activities. The KCU's ICT Policy is a guide on how ICTs shall be used to achieve the goals and aspirations of KCU. It highlights how the usage of ICTs shall be implemented, their development and maintenance, the optimal distribution of resources (hardware, software, data and human resources) as well as the safe and healthy utilization of ICTs and the environment. This policy seeks to enumerate the rules necessary to ensure the existence of the highest levels of consistency, control and harmonious interaction with ICT.

2. POLICY STATEMENT

2.1. Information and Communication Technologies facilities are simply electronical and mechanical tools that facilitate the storage, manipulation, analysis and transfer of information.

2.2. KCU is committed to providing safe, effective and efficient usage of ICT facilities by KCU stakeholders (Academic and Administrative Staffs, students, Guests).

2.3. KCU is committed to training graduates to develop innovative ICTs that provide more secure, efficient and effective solutions to the contemporary global challenges.

3. GUIDING PRINCIPLES FOR THE IMPLEMENTATION OF THE POLICY

3.1. The Directorate of Library and ICT Services demonstrates an on-going commitment to mainstreaming ICT usage by ensuring that the relevant policies, practices, metrics are in place. Frequent and consistent communication will be issued by the Directorate of Library and ICT Services about tips on how to execute safer, more secure and efficient operations. This will be broadcast to the affected or target audience(s).

4. MAINSTREAMING DIVERSITY

4.1. KCU supports diversity and does not discriminate against minority entities based on age, gender, race, sexual orientation, religion, political affiliation, e.t.c. Diversity is encouraged in the different spheres like educational preferences, research interests, funding preferences, work-life-balance, performance management, career management and other inclinations or variations.

5. EDUCATION, TRAINING AND KNOWLEDGE BUILDING

5.1. KCU is committed to continuously re-tool, educate and train all employees, lecturers and administrators in order to improve on institutional practices.

5.2. KCU operates in an open and flexible environment and welcomes people from diverse backgrounds. The work culture at KCU is based on the principles of hard work, creativity, fairness and resource optimization.

5.3. KCU is committed to fair, transparent and competitive recruitment and promotion of personnel. KCU will adopt policies that enable all employees of KCU to develop satisfying careers, following the regulations given in the Appointments and Promotions policy.

5.4. KCU seeks to develop relationships with a range of partnering institutions in order to advance mutual interests and to further the development of internal knowledge and capabilities.

6. KEY ICT POLICIES

6.1. The KCU ICT Policy contains the following

policies,: 6.1.1. Acceptable Use Policy

6.1.2. Electronic Mail Policy

6.1.3. Anti-virus and Anti-Spam Policy

6.1.4. User Password Policy

6.1.5. Data Backup & Restoration Policy

6.1.6. Software Use Policy

6.1.7. Internet Bandwidth Policy

7. ACCEPTABLE USE POLICY

7.1. The purpose of this policy is to ensure the proper use of KCU's ICT facilities, software, services and systems by its employees (academic and administrative), guests and students 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.

7.2. This acceptable use policy has been drawn up with the following objectives:

7.2.1. To encourage the use of both the Internet and hardware as a conduit

for free expression without infringing the rights of others;

7.2.2. To protect and preserve the privacy of individual users and the public at large;

7.2.3. To discourage the irresponsible use of hardware and network resources, which use may result in the degradation of service;

7.2.4. To ensure the security, reliability and privacy of KCU's system and network infrastructure;

7.2.5. To avoid situations that may result in the occurring of any form of civil liability;

7.2.6. To propagate the image and reputation of KCU as a reliable and responsible University;

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

7.4. KCU reserves the right to monitor and record all activities related to University activities using ICT facilities, software, services and systems.

7.5. The Directorate for Library and ICT Services is responsible for the following:

7.5.1. Monitoring network traffic and activities related to University activities;

7.5.2. Recording all activities related to University activities;

7.5.3. Putting in place measures to ensure security, reliability, fair use and free expression of users without infringing the rights of others;

7.5.4. Ensuring availability of measures to protect and preserve the privacy of individual users and the public at large;

7.5.5. Disseminating information to sensitize users on irresponsible acts in the use of hardware and network resources, which use may result in the degradation of service; and

7.5.6. Promoting safety of users and network infrastructure.

8. ELECTRONIC MAIL POLICY

8.1. As a University, KCU commits to provide the members of her community an electronic communication infrastructure that includes computing resources, network connectivity, and software tools for electronic communication. The KCU's community is reminded that use of e-mail is a privilege, not a right and should be treated as such by all users.

8.2. All e-mail communications (and associated attachments, objects, graphics, videos) transmitted or received by KCU network are subject to the provision of this policy, regardless of whether the communication was sent or received on a private or KCU owned computer.

8.3. The Directorate of Library and ICT Services is responsible for the following:

8.3.1. Creating email addresses for new members of the KCU community. This also includes access rights e.g. passwords, biometrics, secret questions, e.t.c;

8.3.2. Disabling email addresses for ex-members of the KCU community. In order to allow smooth transition, this will be done after a period of three months;

8.3.3. Monitoring the electronic mail management usage by its users in a regular or systematic manner. Such monitoring may include tracking addresses of e-mail sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages. Please note that DIQL reserves the right to monitor such usage from time to time and without prior notice; and

8.3.4. Minimizing any misuse or illegal use of email communications.

8.4. The mailbox owner is expected to:

8.4.1. Be responsible and liable for all messages sent from their e-mail accounts and ultimately responsible for all activity performed under their account;

8.4.2. Keep his password secret e.g. by not disclosing it out to another person,

frequently changing it, not writing passwords down or using any other processes that facilitate automatic log-on;

8.4.3. Use only e-mail accounts that they are authorized to use;

8.4.4. Use email accounts for legal, moral and authorized activities, e.g. by not committing a crime using his/her email account;

8.5. The mailbox owner is expected to regularly carry out some activities to manage email accounts and documents. This includes:

8.5.1. Reading all the new e-mail messages at least once in every 1 or 2 days and replying as soon as possible;

8.5.2. Not letting messages build up in the Inbox and deleting messages as soon they are no longer needed;

8.5.3. Opening the 'Sent messages' folder at least once a week and deleting old messages that are no longer needed;

8.5.4. Saving messages that they want to keep onto the hard disk or removable disk; and

8.5.5. Logging out of the email account before exiting the application.

8.6. Mailbox owners are expected to adopt practices that increase privacy and confidentiality of their email communications. They need to be aware of the following:

8.6.1. E-mail messages may be saved indefinitely on the receiving computer;

8.6.2. Copies of e-mails may be forwarded electronically or printed on paper;

8.6.3. 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);

8.6.4. It may be possible for other people to read or change messages that you send by forwarding it to others;

8.6.5. New e-mail will be prevented from coming in to the mailbox once the mailbox has reached the maximum allowable storage space; and

8.6.6. KCU expects members of its community to exhibit acceptable ethical conduct in the use of computing resources. Users 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.

9. ANTI-VIRUS & ANTI-SPAMMING POLICY

9.1. To ensure that the University will provide its community with adequate protection from computer viruses, unsolicited and unwanted emails. The university shall invest and deploy anti-virus and anti-spamming software on ICT facilities owned or leased by the University as well as on ICT services outsourced by the University.

9.2. The Directorate for Library and ICT Services is responsible for the following:

9.2.1. Installing anti-virus software to ensure that all networked computer servers, computers and notebooks used by the University users are protected against virus infections;

9.2.2. Installing Anti-Spam software that automatically separates suspected spam from regular mail;

9.2.3. Minimizing any misuse or illegal use of email communications; and

9.2.4. Protecting the community against other malicious attacks like denial of service, spy ware, phishing, e.t.c.

9.3. Users of University resources are expected to act in the following way:

9.3.1. Report any case of virus, spam or other security risks;

9.3.2. Refrain from creating or initiating virus and spam attacks; and

9.3.3. Use the existing technologies to minimize effects of virus, spam and other attacks.

10. USER PASSWORD POLICY

10.1. The policy ensures that the user has the minimum standard applied to their user password to support the confidentiality, integrity and security of the University ICT resources. This policy refers to users of university resources that require passwords;

10.2. 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;

10.3. The Directorate of Library and ICT Services is responsible for the providing passwords for access to sensitive or controlled environments like email

accounts, tests and examinations, restricted rooms, sensitive files and folders as well as various gadgets; and

10.4. Password holders are expected to treat all passwords as private and confidential and not to be divulged, shown or given to any party other than the user.

11. DATA BACKUP & RESTORATION POLICY

11.1. 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.

11.2. The Directorate for Library and ICT Services is responsible for performing daily back up for the entire critical corporate database for the entire University and periodically testing the backup disks to ensure they are recoverable.

11.3. The Individual users shall be responsible for backing up their own data which is on their own desktop and notebook computers.

12. SOFTWARE USE POLICY

12.1.To ensure that software that the University provides the service as expected. This includes the financial management software, human resources, academic records and any other software in use.

12.2. The Directorate for Library and ICT Services shall procure the software after approval from the relevant organs and procure software licenses after approval from the relevant organs.

13. INTERNET BANDWIDTH POLICY

13.1.To manage bandwidth, use to avoid degradation and ensure network efficacy. Management of Bandwidth resources shall be entrusted to the Directorate of ICT, Quality Assurance and Library services.

13.2. Internet Bandwidth will not be over utilized as to prevent access to critical information, research and online educational material.

14. POLICY VIOLATIONS

14.1. The procedure that follows after a violation of this policy is reported or noticed is that:

1.1.1.1. The Director of the Directorate for Library and ICT Services will set up a team to investigate the allegation or suspicion. If it is a student being investigated, The Dean of the School he belongs to must be part of this team. If it is a member of staff being investigated, the Deputy Vice Chancellor must be part of this team.

1.1.1.2. The Director of the Directorate for Library and ICT Services will 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.

1.1.1.3. After investigations are complete, the findings will be forwarded to the disciplinary committee, which will decide whether the suspect is guilty or not, and which will determine the disciplinary action to be taken.

15. IMPLEMENTATION AND EVALUATION

15.1. The Directorate of Library and ICT Services is responsible for implementation and evaluation of this Policy reporting to the Vice Chancellor. The key officers will be the Director and ICT System Administrator.

15.2. The Director is responsible for the overall activities of the ICT Directorate and the coordination point for all external support escalation services. He/she liaises with other units regarding annual planning of ICT activities; improvements to hardware and software functionalities; any ICT related acquisitions; all ICT budget decisions; coordination of ICT Strategy and ICT Policy; daily, weekly and other, tasking of all ICT staff; coordination with trainers for, and some delivery of, training regarding ICT Policy related training components.

15.3. The ICT System Administrator reports to the Director and is responsible

for all Server activities including Users, data security (access rights, backups, antivirus, disaster recovery actioning); LAN configuration; Internet usage; Email accounts and usage; direction to Support Desk Manager with ICT Department Manager approval for system additions and changes at User and non-Server locations; maintenance of the Server based components of any computerized information systems; coordination with external support escalation including remote access to Servers by external support escalation entity; requests to ICT Section Manager for Help Desk staff activities relating to non-Server Systems Administration activities; keep Users informed of ICT Policy issues and system usage changes; acquisition requests to ICT Department Manager.