KUMASI TECHNICAL UNIVERSITY

ICT RESOURCES USE POLICY

(I-RUP)

October, 2020

Table of Contents

1.0 Introduction

1.1 Preface

As a public institution of higher education, Kumasi Technical University is committed to fostering an educational climate in which students, lecturers and non-teaching staff can approach their respective roles with a sense of high purpose as well as being able to study and work without obstructions, harassment and intimidations. The ICT Resources Use Policy (I-RUP) recognises that personal viewing or transmittal of potentially offensive digital materials may result in excessive use of campus computer and network resources which is inconsistent with professional responsibilities and ethical standards. Such practices may also result in educational and work environments that are not conducive for academic and research work.

In effect, all members of the University community are advised that the Institution does not condone and will not tolerate any such actions that are proven to constitute excessive use, to create a hostile work environment, or to have the effect of harassing or intimidating members of the University community. In addition, any viewing or transmitting of illegal materials is explicitly prohibited. The University also emphasizes that its policies are not aimed at impairing free expression and open inquiry or unduly restricting access to any lawful digital materials by those who would do so within the guidelines of the I-RUP.

1.2 Scope

This policy applies to all users of the University's information communication technology (ICT) resources, whether initiated from a computer located on or off-campus. This includes any computer and information system or resource, including means of access,

networks, and the data residing thereon. This policy applies to the use of all the University ICT resources whether locally or centrally-administered. It also applies to all users including those with their own devices to access the University's Resources. Administrators of individual or dedicated University resources may enact additional policies specific to those resources, provided they do not conflict with the provisions of this and other official policies and laws. Users are subject to both the provisions of this policy and any other policies specific to the individual systems they use.

This policy is organised into ten Sections:

i. The Computer System

ii. User Authentication and Authorisation

iii. Malicious Software (Malware, Viruses, Spyware, Trojans, etc.)

iv. Email and Social Media

v. The Internet and Intranet

vi. Network Usage

vii. Software Installation and Usage

viii. Physical Security

ix. Computer Lab Access

x. Personal Devices Use Policy (BYOD Policies)

1.3 Purpose

The principal concern of this policy is the effective and efficient use of ICT resources. The primary focus is to ensure that the resources

are used in a manner that does not impair or impede the use of these resources by others in their pursuit of the mission of the University. This policy is intended to ensure:

i. the Confidentiality, Integrity, and Availability (CIA) of the University's resources;

ii. that the user community operates according to established policies and applicable laws;

iii. that these resources are used for their intended purposes; and

iv. that appropriate measures are in place to assure that the policy is honored.

This policy is not intended to prevent or prohibit the sanctioned use of campus resources as required to meet University's core mission, academic and administrative purposes.

1.4 Guiding Principles

The following principles underlie this policy and should guide its application and interpretation:

i. Freedom of thought, inquiry, and expression are paramount values of the University community. To preserve those values, the community relies on the integrity and responsible use of the University ICT resources by each of its members.

ii. ICT resources are provided to support the University's mission, research and learning.

iii. To ensure that these shared and finite resources are used effectively to further the University's mission, each user has the responsibility to:

(a) use the resources appropriately to maintain the confidentiality, integrity and availability of ICT resources;

(b) respect the freedom and privacy of others;

(c) protect the stability and security of the resources; and

(d) understand and fully abide by established University policies and applicable public laws.

1.5 Policy Application

As a general guideline, the Institution regards the principle of academic freedom to be a key factor in assuring the effective application of this policy and its procedures and practices. This policy applies to all end users of KsTU ICT Resources.

All existing laws of the country and the University regulations and policies apply, including not only laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. This may also include laws of other institutions and countries where materials are accessed electronically via the University resources by users within those jurisdictions.

The University reserves the right to limit access to its resources when policies or laws are violated and to use appropriate means to safeguard its resources, preserve network/system integrity, and ensure continued service delivery at all times. This includes

monitoring routing information of communications across its network services and transaction records residing on University resources, scanning systems attached to the KsTU network for security problems, disconnecting systems that will become security threats, and restricting the materials transported across the network or posted on to the University's systems.

1.6 Policy Provisions

This policy is not intended to provide a full accounting of applicable laws and policies. Rather, it is intended to highlight major areas of concern with respect to responsible use of the University's ICT resources.

1.7 Policy Compliance

The ICT Director is authorised by the Vice-Chancellor to ensure that the appropriate processes to administer the policy are in place, communicated and followed by the University community. The ICT Director or designee will ensure that suspected violations and resultant actions receive proper and immediate attention of the appropriate University official, law enforcement, and outside agencies.

The ICT Directorate will inform users about the policy; receive and respond to complaints; collect and secure evidence as required; advise and assist users on the interpretation, investigation and enforcement of this policy; consult with the University's Legal Unit on matters involving interpretation of law, campus policy, or requests from outside law enforcement agencies and/or legal counsel; and maintain a record of each incident and its resolution to inform future policy changes.

1.8 Consequence of Non-Compliance

Where there is a breach of any of the provisions in this policy, the Directorate shall take action upon receipt of formal complaints about a specific incident through the ICT Directorate's helpdesk or through discovery of a possible violation in the normal course of administering ICT resources.

First offense and minor infractions of this policy, when accidental or unintentional, will be resolved informally by the unit administering the resource. This may be done through e-mail or in-person discussion and education.

Repeated offenses and serious incidents of non-compliance may lead to disciplinary action under the University disciplinary policies and procedures for students and employees. Serious incidents of non-compliance includes but are not limited to unauthorised use of ICT resources, attempts to steal passwords or data, unauthorised use or copying of licensed software, repeated harassment, and threatening behaviour.

In addition to the above, inappropriate use of ICT resources may result in criminal, civil and other administrative liability.

Appeals of actions resulting from enforcement of this policy will be handled through existing disciplinary procedures for KsTU students and employees.

1.9 Reporting Irresponsible Use

Suspected violations of this policy should be reported to ICT Directorate at helpdesk@kstu.edu.gh or ict. director@kstu.edu.gh in accordance with ICT helpdesk processes and procedures. There might be situations when the following additional offices/

officials should be notified of suspected violations when filing a complaint:

Deans/Directors, Heads of Department, Assistant Registrars and/or one of the following offices if the incident occurs in the course of employment with the University:

- Registrar's Office
- Human Resources Unit
- Academic Affairs
- Admissions Office
- Legal Unit
- Counseling Unit
- Security

2.0 Computer Systems

2.1 Ownership

The personal computer (PC) is the property of KsTU and is provided to assist in the performance of one's job. Personal use of the computer system is a privilege that shall be withdrawn at any time when found to be misused.

2.2 Appropriate Use

The computer system shall only be used for approved purposes and with authorisation from heads of department. Occasionally, limited and appropriate personal use of the computer system is permitted when such use does not:

i. Interfere with the user's work performance;

ii. Have undue impact on the operation of the computer system;

iii. Violate the provisions of this policy or any other policy of KsTU.

Users are responsible for using computer resources in a professional, ethical, and lawful manner.

Staff must not deliberately perform acts that will waste computer resources or unfairly monopolise resources. These acts include but not limited to:

i. Sending mass mailings or chain letters

ii. Downloading or playing games on the internet

iii. Printing multiple copies of documents

iv. Using large amounts of bandwidth and storage space for audio, video and picture files that are not work related or for academic and research purposes.

v. Using computer facilities to support any non-KsTU business

vi. Using computer facilities for political, religious or promotional activities (including the activities of non-profit organisations)

vii. Accessing or circulating offensive material, e.g. pornography

2.3 Right of Access

The computers and user accounts given to KsTU staff/ students are to assist them in the performance of their jobs. Staff/Students must not have an expectation of privacy in anything they create, store, send, or receive on KsTU computer system (subject to relevant local laws).

2.4 Monitoring and Control

KsTU has the right to monitor and control any aspect of its computer system, including internet activities. This includes:

i. Chat groups, newsgroups and social media platforms

ii. Material downloaded or uploaded by users

iii. Email sent or received.

iv. Sites being visited

2.5 Inappropriate Material

Materials that are fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate should not be sent by email or other form of electronic communication. This policy also applies to material of similar content, downloaded from the Internet, or displayed on or stored in KsTU's computers. Any user encountering or receiving this kind of material must immediately report it to the ICT Directorate.

2.6 Copyright

Staff should not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright laws and applicable licenses that may apply to software files, graphics, documents, messages, and other material you wish to download or copy. No agreement should be made for a license or for downloading of any material for which a registration fee is charged, without first obtaining written permission from the ICT Directorate. Consult ICT Directorate if in doubt.

2.7 Ownership of Information Assets

KsTU retains exclusive right of ownership of all the assets it has procured, including hardware, software and data.

2.8 Third-Party Files

Users should not alter or copy files belonging to other users without first obtaining permission from the owner of the file. The ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy that file.

2.9 Approved Hardware

Procurement of ICT equipment should conform to KsTU standard product list. This covers portable computers, mobile phones, tablets, wireless equipment, and removable storage devices. All equipment must be registered with KsTU and must be authorised by Works and Physical Development Directorate, assigned asset tags and signed for, as an asset by each user. On leaving the direct employment of KsTU or its services, all equipment must be returned and signed-off by end user and the appropriate authority (Works and Physical Development Directorate).

2.10 Approved Installation

Software and hardware must only be installed on computers by ICT Directorate in conformity with the Software Management and Usage Policy.

2.11 Licensing

Every staff is responsible for ensuring that software installed on his or her personal computer is properly licensed in conformity with the Software Management and Usage Policy.

2.12 Unauthorised Software

Unauthorised software is subject to removal from an employee's personal computer. The procedure shall involve initialising the computer and the loss of personal settings.

2.13 Encryption Software

Users should not install or use encryption software on any KsTU computers without first obtaining written permission from the ICT Directorate.

2.14 Theft or Loss

In the event of theft or accidental loss of any computing equipment, including portable devices, the Head of Security and ICT Directorate helpdesk should be contacted immediately.

2.15 Physical Security

All KsTU computer systems must be protected in a reasonable and appropriate level of physical security. Laptops must be secured with locking devices in KsTU offices and elsewhere.

2.16 Access to Third-Party Networks

A user's ability to connect to third-party computer systems through the University's network or by a modem does not imply a right to connect to those systems or to make use of those systems (unless specifically authorised by the operators of those systems). Non-compliance with this policy can compromise confidential information. In the case of external systems, unauthorised access can lead to criminal prosecution. This makes our systems vulnerable to cyber threats.

2.17 Security Circumvention

Users shall not

i. attempt to circumvent KsTU's security measures to uncover security loopholes.

ii. gain or attempt to gain unauthorised access to secured or protected files on the computer system.

iii. tamper with any software protection or restrictions placed on computer applications, files or directories.

Users who engage in this type of activity shall be subject to immediate termination of their user access.

Where exemptions to this policy may be necessary, approval must be obtained from the ICT Directorate.

2.18 Screen-Lock Unattended Workstations

Workstations must be locked when unattended. Note: Screensaver only appears automatically after some minutes of inactivity. If sensitive data is displayed on your screen (e.g. questions, report, etc.), prior to stepping away, force the system to lock by pressing **Ctrl-Alt-Del** (and choose "**LOCK** this Computer").

3.0 User Authentication and Authorisation

3.1 Sharing User Identification (ID)

A single-user ID shall not be shared amongst multiple individuals.

3.2 Borrowing ID

It is prohibited to access another person's user account or password.

3.3 ID Authorisation

All requests for user account creation must be authorised by staff designated by KsTU. This also applies to requests for re-enabling, disabling, or changing capabilities of user IDs.

3.4 ID Permission(G)

Assignment and re-assignment of permissions (to use software applications, directories, files, etc.) must be authorised by the Line Managers or Heads of Department or Deans/Directors and an authorised ICT Directorate representative. Authorisation from designated KsTU staff is required before ICT personnel are permitted to create or modify User Groups-granting access to institution's data.

3.5 Role Changes

Staff members are responsible for notifying ICT Directorate of changes to their roles which may necessitate altering permissions or publishing information on any of the websites.

3.6 Privileged IDs

Request for a Privileged ID such as Domain Admin must be supported by a business case. In the creation of a Privileged ID, authorisation should come from both ICT Director and Head of the department under which the system is managed.

3.7 Deleting Accounts

User account information for disabled or inactive accounts (including dormant accounts) must be removed from the system after a period of three months unless the business application and/or software requires otherwise.

3.8 Password Requirement

Access to all devices (laptops, desktops, tablets and mobile phones), as well as to critical business applications must be restricted by means of access code (user ID and password). Access should be provided only to authorised users. Systems that must carry password protection include:

i. Wireless network (Wi-fi)

ii. Windows login

iii. Finance software

iv. Network and intranet services

v. (https://isp.kstu.edu.gh/)

vi. Email access (https://mail.kstu.edu.gh)

Any other software at KsTU

3.9 Password Safeguarding (G)

Passwords must remain confidential. Users are responsible for safeguarding their own ID and password, and are responsible for all transactions made using their username and password. Users should follow these policies to safeguard passwords:

i. Do not store passwords and user IDs together.

ii. Passwords must not be printed, stored online, written down, or given to others. If it is necessary to store a password online, it must be kept in encrypted form.

iii. Do not store passwords on stickers under keyboards or near their workstation.

iv. Passwords must not be emailed in clear text form over the internet, via public networks or wireless devices.

v. Users must change the initial or default password provided during set-up or first installation of a system.

vi. Passwords must be changed every 90 days. Most systems force this change but users must be aware of the requirement (should be able to perform prompt messaging)

vii. Passwords must be changed whenever there is a risk that they have been compromised.

Note: Never use your KsTU ID or password for non-KsTU systems.

3.10 Password Format

Password format must:

i. Be a minimum length of eight characters

ii. Include at least one uppercase alphabet character

iii. Include at least one lowercase alphabet character

iv. Include at least one 'special' character, e.g. % or !

v. Have no more than three (3) consecutive characters from a previous password

vi. Not consist of words found in the dictionary

vii. Not contain the user ID as part of the password

viii. Be different from the user's previous five (5) passwords

Note: Some systems will not allow passwords that comply with all of the above, in which case comply as far as possible.

3.11 User's Security Information

Users must provide Helpdesk with secret information that can be used to verify their identity when requesting a password-related action.

3.12 Right to Inspect

KsTU has the right to inspect without prior notice all material stored on its computer system (in accordance with local laws and regulations). KsTU has access to all material stored on its computer systems regardless of whether material is encoded under a particular user's password.

4.0 Virus, Spyware, Malware

4.1 Spreading Virus

Files obtained from sources outside of the KsTU network could contain damaging computer virus. This includes external storage brought from elsewhere; files downloaded from the internet, from newsgroups, facebook or other online services; files attached to email and files provided by students, contractors, suppliers and external consultants. All approved external storage devices should be scanned by KsTU approved anti-virus software. If you suspect that a virus has been introduced into KsTU's network, notify ICT Helpdesk immediately.

4.2 Antivirus Software

All KsTU computers must have anti-virus protection software installed before connecting to the network. Users must keep anti-virus software updated and must not disable or alter its configuration. When instructed to update anti-virus software, users must do so promptly. Users are required to notify ICT Directorate in the event that any computer's antivirus is not updating.

4.3 Antivirus Software Updates

If you use movable computers (laptops) and are on leave, you should make it a point to be on site to update your anti-virus software periodically. You are to remain logged on till the update is completed.

4.4 Internet Software

Do not install software or download files from the internet that are not absolutely necessary for KsTU business. This especially includes video tutorials, music, freeware, shareware and games.

4.5 Email Attachment

Email attachments and other files obtained externally must be treated with caution. Never open files of suspicious nature from unknown senders. If a file appears to be transmitted from a known sender, be sure the source is genuine. Emails of suspicious nature must be deleted. If you are not sure of the safety of an email, contact Helpdesk for directions as to how to get rid of the file.

4.6 Macros in Documents

Disable 'macro' functions in documents sent from third parties, if they are not known to be a secure source.

5.0 Email and Social Media

5.1 Truthful Communication

Anything created or stored on the computer system might be reviewed by others. Staff must endeavour to make each electronic communication truthful and accurate. Use the same care in drafting email and electronic documents as you would for any other written communication.

5.2 Litigation

Emails and information on social media platforms can be used as evidence in a lawsuit and therefore, users should be particularly careful about:

i. Distributing messages more widely than it is necessary.

ii. Expressing opinions about matters beyond an area of expertise.

iii. Making statements which could be interpreted as implying that the Institution is doing something unlawful.

5.3 Information about Other Institutions

Do not include information about other institutions, unless this is necessary for formal reasons. When necessary, make sure information is factual and accurate. Avoid opinionated statements.

5.4 Contractual Obligations

Do not use email to create legal or contractual obligations without authorisation from Management. Be aware that legal commitments can be created even in informal expressions.

5.5 Data Protection

Data Protection regulations exist in many territories to restrict the handling of information about individuals. Users must not infringe on these regulations. Consult the HR Department if you are unsure of how this affects your work.

5.6 Use of 'KUMASI TECHNICAL UNIVERSITY' or 'KsTU' in Chat Rooms and Social Media

Do not refer to KsTU or any of our Institutions names in anything published through the internet (e.g. Facebook, whatsapp, twitter, skype, yahoo messenger, discussion group, etc.) without being in authority to do so.

5.7 Phishing, Vishing and Smishing

i. No user should try to acquire other user's passwords or account (Phishing) for any reason.

ii. No user should try to get other users system's account through phone (Vishing) for malicious activities.

iii. No user should try to get other user's systems account through SMS messages (Smishing) for any malicious intentions.

5.8 KsTU Mail Domain

Sending mass emails from the kstu.edu.gh domain is not permitted. It consumes resources, increases the likelihood of spreading viruses and invites attack against the Institution's primary email system.

5.9 Spoofing

Users should not under any circumstances disguise their identities in sending messages. Identity disguise or 'spoofing' is often used to hide the identity of a person committing unauthorised and malicious acts.

5.10 Spam Filtering

KsTU filters incoming email and deletes unsolicited commercial 'junk mail' (i.e. spam) before it enters the KsTU's system. Should some junk mail pass through our filtering mechanism:

i. Do not visit URLs listed in junk mail messages

ii. Do not assume the "FROM" address to be correct

iii. Do not respond to the message, even to request removal from a mailing list

iv. Do not buy products or services from junk mail advertisements

5.11 Chain Letters

Do not participate in chain letter schemes. These waste valuable bandwidth and send unwanted email to other users.

5.12 Forwarding Messages

Do not forward a message without express or clearly implied permission to do so. Do not alter the content of a third party's message, when forwarding it.

5.13 Sending Attachments

Before sending someone an attachment such as a picture or any other type of file, let your recipient know what to expect via a preliminary message. If you do not know the recipient personally, send an email requesting permission to send the attachment.

5.14 Space Constraints

It is important to manage mailbox size. Email messages and attachments stored on the server consume tremendous amounts of space. As messages accumulate, system response time will deteriorate.

These policies are in effect to manage mailbox size:

i. Emails should not be stored with attachments. If retention of an attachment is necessary, it should be saved to a folder and stored outside the email system.

ii. Emails that do not need to be kept must be deleted in accordance with KsTU Records Retention Policies.

5.15 Inappropriate Mail

Do not send messages or any material that could reasonably be construed as defamatory, discriminatory, threatening, harassing, obscene or otherwise offensive or illegal.

6.0 Internet and Intranet

6.1 Responsibility for Internet

Internet users must exercise care as it is sometimes difficult to avoid contact with materials which may be offensive, sexually explicit or inappropriate

6.2 Approved Internet Connections

Staff must only connect to the internet via approved KsTU network systems, utilizing approved web filtering software. For further information on approved network systems, contact ICT Helpdesk.

6.3 Internet Games

Staff should not use KsTU's internet connection to play games or download entertainment software, including non-KsTU created screen savers.

6.4 Keeping Email Address Private

Individual KsTU email addresses should not be published on public sources such as internet bulletin boards, distribution lists, or web pages as this could be used for spamming.

6.5 Chat Rooms and Social Media

Never use chat rooms or other social media like the facebook and twitter during working hours, unless it is for academic purposes. Do not make reference to KsTU's official documents and data, or otherwise share confidential or restricted information when participating in internet bulletin boards, chat rooms, and other social network.

6.6 Downloading Executable Files

Downloading and installing executable files from the internet is not permitted. Contact the ICT Directorate if you need any software.

6.7 Internet Certificates

Users may sometimes visit websites offering an 'authority certificate'. Unless this is being offered from a legitimate KsTU site, certificates must be refused. In accepting such certificates, your browser will extend trust to all sites signed by that authority.

7.0 Network Usage

7.1 Protecting Data Ports from Guest

KsTU students and staff are responsible for ensuring that outsiders (guests) do not plug non-KsTU equipment into the office network ports. The ICT Helpdesk should be contacted to obtain guest connectivity information if it becomes necessary.

7.2 Access Approval

Access to the KsTU Local Area Network (LAN) and the Wireless Network by non-KsTU staff with non-KsTU equipment requires approval by the ICT Directorate.

7.3 Approved Equipment

Access to the network is only permitted using KsTU owned, supported or approved computers, tablets or smart phones (for staff). Any exceptions must be assessed by KsTU ICT Directorate.

7.4 Approved Remote Access Solutions

Remote access to KsTU's network must be performed using only solutions approved by KsTU's ICT Directorate. Contractor and consultants should receive clearance before using our remote access connections.

7.5 Personal Firewalls

Computers accessing KsTU's network remotely, via a broadband connection or VPN, must have firewall installed on their computers. If you are not sure of the procedure to do so, contact ICT Helpdesk.

7.6 User's Accountability

All remote users are accountable for activity resulting from their ability to remotely access KsTU systems. Unique Network and Server credentials must be used and the sharing of passwords is not permitted.

7.7 Simultaneous Connections

Your computer must not be connected to the KsTU network and at the same time to another non – KsTU network.

7.8 KsTU Data on Non KsTU Systems

Users that access KsTU's networks using non-KsTU computers must protect KsTU data stored on those machines in accordance with this policy. (Refer to 11.0 on BYOD).

7.9 Network Testing

Network testing, 'sniffing', 'eavesdropping' and penetration testing by non-ICT staff members are not permitted unless explicit approval is granted by the ICT Director.

7.10 Wireless Access Points

Wireless access from KsTU sites to the corporate network must use Wireless Access Points on a dedicated Wireless LAN approved by the KsTU ICT Directorate. User account for wireless network should

not be shared with or transferred to third parties.

7.11 Bluetooth

Use of wireless technology, such as Bluetooth and WiFi, has become popular for short distance wireless connectivity (e.g. phones, tablets, printers, etc), yet it must be recognized that it has security weaknesses. Use of Bluetooth technology for remote connectivity to the KsTU Trusted Network is not permitted, and approval must be sought from the ICT Directorate.

The user must be familiar with the technology's current weaknesses and know how to ensure secure use of Bluetooth devices.

The user must take these precautions:

i. Device must be switched to non-discoverable mode when Bluetooth use is not required

ii. A device's security options must be turned on, and PIN codes used, with eight or more alphanumeric characters

iii. Devices must be paired in private areas

8.0 Software Installation And Usage

8.1 Software Installations

All system software shall be installed by ICT Directorate or with ICT Directorate. This is to ensure that any of the policies will not be violated (copy right issues, virus propagation etc.). This is also to make sure that the requirements for the software in terms of machine specifications are met to enhance the usage of that software.

8.2 Software Use

All software shall be used for the purpose that it was procured. All educational license software shall be used as such. Staff must not remove or delete software. Removal or deletion of software must be done only by Systems Administrators in the ICT Directorate.

8.3 Storage of Software

All the Institution's software or copies of the software including licenses and manuals shall be kept by the ICT Directorate in a fire proof safe as stipulated in the Disaster Recovery Plan (Backup Policy).

8.4 Software Audit

KsTU reserves the right to inspect staff computer system for violations of this policy. The ICT Directorate will conduct regular audit on all KsTU's computers (including portables) and servers, to ensure that KsTU is in compliance with all software licenses. Periodic, random audits shall also be conducted as appropriate. Audits will be conducted using an effective auditing software or procedure in a manner that is the least intrusive and disruptive to staff. The full cooperation of all users is required during audits. (Refer to Software Management and Usage Policy).

8.5 Procurement of Software

All computer software shall be procured in consultation with the ICT Directorate. This is to provide technical advice to the user department and the Institution as a whole in terms of machine specification, network connectivity, system security and functionality, as well as storage capacity. (Refer to Software Management and Usage Policy).

9.0 Physical Security

9.1 Directories

Internal directories or telephone books or other guides that identify the location or telephone numbers of secure and sensitive areas must not be made accessible to the public or unauthorised persons. Unwanted papers should be shredded.

9.2 Locking Device for Portables

Portable computers must be physically attached to desks with security cables, to prevent theft.

9.3 Taking Portable Computers Off-Site

Certain circumstances demand that portable computers be taken off-site or overnight. These devices must be kept securely under locks.

9.4 Safe Storage Overnight

Portable computers left in the office overnight must be stored in locked cabinets.

9.5 Labeling Portable Computers

Portable computers must bear an easily visible label specifying "Property of KsTU" (e.g. Asset tag), so that it can be tracked, to avoid theft or accidental loss.

9.6 Vigilance at all Times

Equipment and media taken away from KsTU premises must not be left unattended. When travelling, portable computers must be carried as hand luggage, and wherever possible, concealed.

9.7 Asset Register

Hardware assets must be logged on an asset register held by the ICT Directorate and Works and Physical Directorate. The ICT Directorate and Works and Physical Development Directorate will authorise permanent removal of an ICT asset from KsTU premises.

9.8 Return of Equipment

Staff or contractors must return all portable equipment belonging to KsTU, upon their permanent departure from KsTU. It is specifically forbidden to allow staff leaving KsTU to retain equipment as part of a termination agreement unless other policies specify so for a particular position or staff.

9.9 Switching Off Equipment

All computer systems such as computers, UPS, printers, scanners should be switched off after close of work or unattended.

9.10 Lock Away Confidential and Restricted Information

All confidential and restricted information on external storage media and paper must be locked securely when unattended.

9.11 Clearing Printers and Copier Papers

Ensure that sensitive documents are not left in printer trays. Clear printer and copier machines of confidential papers as soon as they are printed.

10.0 Computer Laboratory Access

10.1 Lab Users

The Computer Lab aims to provide basic, functional computer services for student and other users who may not have access to such technology on their own. The Computer Lab provides an environment where students go for practical work. KsTU computer labs are open to all students, lecturers, and staff.

10.2 Saving Documents

Users are permitted to save files to the local hard drive at their own risk. The Computer Lab is not responsible for any files that are lost, stolen, or deleted. Users are encouraged to back up their files by using their own flash drives.

10.3 Safety of Personal Items

Users are responsible for their own possessions and belongings. The Computer Lab staff are not responsible for personal items that are lost or stolen while in the lab.

10.4 Personal Manners at the Lab

The consumption of foods and beverages, including water is prohibited. The Computer Lab is a quiet area. All cell phones must be silenced while in the Computer Lab. Students must refrain from having group meetings and cell phone conversations in the lab, as they are a distraction to other users. If deemed necessary, a member of the Computer Lab staff may ask you to leave.

10.5 Fault Reporting

If any computer equipment malfunctions, users should not attempt to repair it. The lab attendant must be notified immediately.

10.6 Installation of Lab Computers

Users are prohibited from installing software on any computer in the Computer Lab (except demonstration labs). If additional software is needed on the computers, the ICT Directorate's Helpdesk must be notified. Only academic applications are supported on lab machines.

10.7 Usage of Computers

All computers in the Computer Lab are for academic, instructional and research purposes ONLY. Using school-related equipment for commercial gain is strictly prohibited and may be subjected to disciplinary actions. All computer lab users must show respect for the lab facility and other users when printing, especially from the internet. Printing is limited to what is deemed necessary for class assignments by the computer lab staff.

10.8 Peer Monitoring

The Computer Lab provides an open academic research environment where students, lecturers, and staff can access scholastic information. It is therefore the responsibility of every user to ensure that the Computer Lab equipment is not being abused, damaged, or used in a manner other than what it is intended for. All abuse should immediately be reported to the Lab Assistant on duty for further action.

10.9 Computer Lab Assistance

The Lab Assistant is available to assist lab users with electronic media, hardware and software issues during normal operating hours. The computer lab staff shall assist with basic applications, internet and printing questions.

During open lab hours, Computer Lab Assistants are responsible for the basics of maintaining the integrity of the Lab's computer network and providing enduser support for network access, printing, and basic application assistance. For more complex issues that cannot be resolved by Computer Lab Assistant, they are instructed to forward the issue to the Computer Lab Coordinator or ICT Directorate. They are not an alternative for learning the necessary applications. For extensive assistance with specific applications, users should consult the appropriate documentation or see their instructor for training assistance.

10.10 Priority

The computer lab facilities have been established for the educational benefit of the students of KsTU. The following covers questions that individuals may have about their rights as users of the computer equipment in the computer labs and can be used to determine priority. Priority for use of equipment in the computer facilities will be administered on a space available basis for educational purposes using the following criteria:

1st Priority – KsTU students with valid ID, who require the use of lab computers to complete their course assignments, grant applications, or other academic activities.

2nd Priority – Other KsTU students with valid Student ID.

3rd Priority – Lectures, administration, and alumni creating job applications.

Internet Relay Chat, and in most cases, e-mail are not considered course-related activities. If the Computer Lab begins to fill up, time limits will be set for Internet social network (facebook etc.) and e-mail use. If the Computer Lab is full, recreational computer users will be asked to vacate their computer stations to allow other students to complete class assignments.

10.11 Software Licensing

Computers are configured according to the needs of students, lecturers and staff. Suggestions for a hardware or software changes should be submitted to ICT Helpdesk by talking with a Lab Assistant. Only software owned by or licensed to KsTU shall reside on campus lab computers. No software or "freeware" shall be installed on any of the lab computers without consent from the ICT Directorate.

10.12 Closing

A Lab Assistant shall give users an official notification to finish up work at 15 minutes before closing. At closing, the Lab Assistant will announce to all remaining users that the Lab is now closed. Users should be ready to leave at the closing time. In the event users are reluctant to leave the lab after it has closed, Lab Assistant shall switch printers and computers off without notification.

11.0 Personal Devices Use Policy

11.1 Bring Your Own Device (BYOD) Guidelines

i. Users of BYOD shall be allowed to use the ICT Resources if they adhere to the content of this policy document and follow basic best practices.

ii. Users shall set BIOS passwords for all computing device such as desktop and laptops computers, set PINS for tablets and smart phones. (G)

iii. Passwords set for all BYOD should conform to the password policy as outlined in the Technical University's Security Policy.

iv. Users shall set screen locks and automatic screen locks to ensure that BYOD lock automatically when not in use.

v. Users shall ensure that all BYOD software/firmware are kept up to date with current version.

vi. Users shall ensure that any encryption facilities on the BYOD are activated if available.

vii. Users shall maintain an effective antivirus on all BYOD where applicable.

viii. Users must delete all data and information stored on the BYOD, thus if they are no longer required.

ix. Users must remove all information from BYOD and set the device to its factory settings before the device is sold, exchanged or disposed off.

x. Any BYOD found to have breached the manufacturer's security mechanisms, such as firewall settings shall not be supported, and ICT Directorate have the right to deny the device access to KsTU information resources to reduce the cyber risk on the Institution's network.

11.2 Roles and Responsibilities

i. The user is responsible for the BYOD and should not leave it unattended. The user is responsible for any unauthorised access or misuse that may occur at the hands of a 3rd party with or without the knowledge of the user.

ii. The user is responsible for enabling passwords and PINs protection on the BYOD.

iii. It is the responsibility of the user to enable configuration and encryption functionalities and the storing of passwords in a safe and secure manner.

iv. The user is responsible for changing the password immediately on discovery that the password has been compromised and report to helpdesk for appropriate actions.

v. The user is responsible for all data and systems backups and recovery.

vi. It is the responsibility of the user to familiarize themselves with the Standard Operating Procedures on handling, storing and transferring data.

11.3 Monitoring of BYOD Devices

i. It is mandatory for anyone using a BYOD to comply with the other ICT Policies. Where non-compliance is identified, ICT Directorate will take appropriate action, which may result in the BYOD being prevented from the University's network.

ii. Routine and un-announced checks may be made by ICT technical support staff to ascertain the level of compliance to the policy. The support team shall report their findings to Director of ICT of any breach of its Policies and may instruct the user to take corrective actions or face disciplinary actions.

12.0 Policy Exceptions

i. In the event of an exception that is not addressed by this Policy, the matter will be referred to the Head of Infrastructure Unit.

ii. The Head of Infrastructure Unit will carry a needs assessment and make a decision based on the assessment.

iii. The Director of ICT will approve or disapprove of the request based on the recommendations from the Head of Infrastructure Unit.

13.0 End-User Agreement Procedure

Users who have been given access to use any of the Institution's assets shall be required to complete an end-user agreement form.