UNIVERSITY OF TECHNOLOGY AND ARTS OF BYUMBA

EDUCATIO-SCIENTIA-MINISTERIA

Post Box: 25, Byumba, Gicumbi District
Northern Province, Republic of Rwanda
Phone: +250 – 789 350 053
Email: info@utab.ac.rw
Web: www.utab.ac.rw

ICT POLICY

Academic year 2016

TABLE OF CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

1) GENERAL INFORMATION

1.1. Introduction and Context

Academic Freedom is central to the mission of higher education. Therefore, University of Technology and Arts of Byumba respects and encourages the free exchange and debate of ideas, including electronic interchanges and all manner of electronic inquiry and publishing in a manner that complies with UTAB's vision and mission. Within this context, UTAB provides access to computing and communications resources to students, staff and the community to support its mission:

- To provide quality higher education and community oriented research
- To shape a skilled workforce in the domains of technology and arts
- To promote a culture of excellence and innovation for quality service delivery

The use of these resources should follow the same standards of common sense, courtesy, and restraint in the consumption of shared resources that govern the use of other UTAB facilities and services. The protection of confidential, sensitive, and proprietary information is critically important to UTAB. Therefore, it is essential that students, faculties, staff and administrators take steps to appropriately safeguard such information. Such safeguards must recognize UTAB community members' rights of free speech, free inquiry and access to one's own information.

UTAB does not condone messages of hate, bigotry, violence or intimidation directed at any individual or group, or harassment of any kind. Allegations of such harassment or threats will be thoroughly investigated by UTAB. If such allegations are verified UTAB will take corrective pursuant to its policy.

UTAB operates a complex data processing environment in two Campuses in Byumba and one Distance and Open Learning Facility at Kiramuruzi. The use of modern information technology entails both benefit and risk. This policy is designed to reduce those risks to an acceptable level and to maximize the benefits to all users. Importantly, this policy are not intended to "lock down" UTAB's information resources and systems to authorized users, but rather provide reasonable protection so that information can be shared appropriately and employed effectively

in the pursuit of the University's goals. This policy will help ensure the confidentiality, integrity and availability of information and information technology resources for all members of the UTAB community.

1.2. Issuing authority

The Directorate of Information and Communication Technology at University of Technology and Arts of Byumba (UTAB)

1.3. Scope

This policy and its supporting documents apply to all users of the information technology environment at UTAB, including the staff, students, contractors, vendors, business partners and other members of the University community. This group, for the purposes of this policy, is referred to as Users. For the purposes of this policy, the entirety of UTAB information technology environment and the information and data therein is referred to as Computing and Communications Resources. Computing and Communication Resources include, but are not limited to computers, networks, software, databases, information and records, services, facilities and access methods.

1.4. Sanctions

It is the responsibility of each User to understand his or her privileges and responsibilities under this Information and Communication Technology Policy and to act accordingly. Users failing to abide by this policy may be subject to corrective action up to and including, dismissal, expulsion, and/or legal action by UTAB. While technical corrective action, including limiting user activity or removing information, may be taken in emergency situations by authorized ICT staff, other corrective action, technical and/or non-technical, will be taken in accord with applicable UTAB policies and procedures.

1.5. Exceptions

Exceptions to the ICT Policy will only be granted if an appropriate justification for the exception is approved and the person responsible for that area of information management or the appropriate Information Administrator accepts the additional risk and/or responsibilities posed

by the exception. To apply for an exception to an Information and Communication Technology Policy, the requestor will prepare a written request for the exception along with a justification and deliver the request to the Directorate of ICT for consideration. The official will advise the requestor on alternatives that comply with the policy.

2) COMPUTER AND OTHER ICT RESOURCES USAGE

2.1. Acceptable practices

1) Computer laboratories may require mobile phones be set to vibrate, but may not require them to be turned off.
2) The computer equipment and resources provided by the University to its staff, students and associates remain UTAB property at all times, including equipment acquired by the UTAB from research funding and research contract funding.
3) Users must log-off in times of absence from a shared computer to avoid improper and/or illegal use;
4) Computing facilities are provided for use by staff in the course of their employment and by students in the course of their education. While other incidental and occasional use may be permitted, such use must not interfere with the employee's work or the student's study. Any abuse of such permission will be treated as a contravention of these regulations.

2.2. Unacceptable practices

The following practices are prohibited:

1) Obtaining without authorization the access codes and/or passwords of another user;
2) Sharing logon usernames with or disclosing passwords to any third person(s) or providing access to any of the UTAB's computing facilities to those not rightfully due such access; this practice is however allowed for centralized service facilities who need to share an account to access the computer;
3) Damaging or deleting files of another user;
4) The use of flash disks, floppy disks and any other device that may possibly be subject to viruses;
5) Using UTAB computing facilities to place, disseminate or receive materials which discriminate or encourage discrimination on the grounds of gender, sexual orientation,

disability, race or ethnic origin except for registered research purposes approved by the competent University organ;

6) Using the UTAB's computing facilities for placing or distributing advertisements relating to any course of business other than those promoting the UTAB's teaching and research activities or its own trading operations;
7) The use of any computer resource to promote any business or enterprise, except that of UTAB, unless such use is explicitly permitted by an agreement between the employee and UTAB;
8) Any action that would impair the function or security of UTAB's computer facilities;
9) Any purposes that could reasonably be expected to cause directly or indirectly excessive strain on any computing facilities, or unwarranted or unsolicited interference with others;
10) Making, storing or transferring unlicensed copies of any copyright or trademark work including computer programs;
11) Accessing social media, like **Facebook**, **Twitter**, **WhatsApp**… for personal use while at work.
12) Using without permission the company name, logo, trademarks, copyrighted information or other intellectual property in blogs, discussion boards or other social networking sites that can infringe on the University's rights to and control over these assets.
13) Using one's university email address or a username for personal matters.
14) Using a company computer, network, personal digital assistant or smartphone to access social media, with risks of introducing possible malicious software or other rogue applications, especially for social media that involves accessing or downloading files.
15) Sending communications over social media that the company is not able to retain for its own records maintenance requirements.

3) EQUIPMENTS SECURITY

1) It is the responsibility of each user to secure his/her ICT equipments while at the work place;

2) Employees who wish to use UTAB's equipments out of its boundaries must submit a request to the Vice Chancellor for approval;

3) Nobody is allowed to make any kind of intervention or repairing. This is reserved to ICT staff only;

4) DATA BACKUP AND RESTORE

1) All ICT backup and recovery procedures must be documented, regularly reviewed and made available to UTAB personnel who are responsible for performing data and ICT system backup and recovery.
2) Access to the on-site backup location and storage safe must be restricted to authorized personnel only.
3) All backup media must be protected with a password and appropriately labeled with date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All passwords should be kept securely at all times by concerned staff;
4) Backups occur regularly as follows:
   - Daily backups take place on a daily rotation;
   - Weekly backups take place on a weekly rotation;
   - Monthly backups that occur the last calendar day of the month and are on a twelve month rotation;
5) Special backups may be made for longer retention periods during special situations such as system upgrades and major projects;

5) NETWORK USAGE

5.1. Definitions

a) Network infrastructure

It is the collection of elements that provide the mechanism to carry out electronic data, voice, and video communications. This includes cabling, switches, routers, computers, software, other network components for wide-area/local-area and wireless network hardware such as wireless access points and their associated components operated within the boundaries of UTAB.

b) UTAB network information services

They are the information and transactional services that UTAB makes available for use via its network and/or the Internet. Examples include e-mail services, Web applications, online course management, etc.

5.2. Eligibility for network access

Only UTAB Staff, students and partners are authorized to use UTAB's network resources. The procedures for getting a network access are as follows:

1) Network access may be requested from the staff of ICT Directorate (Director of ICT, Website and Database Manager, Website Content Manager and Computer lab Attendant) upon the presentation of a student ID card or Employee ID card and registration of the device to be used on the network.
2) Individuals who are not members of the UTAB community pay for internet services.
3) Students have free access to internet in computer lab upon request by the lecturer. The later determines the time to be allocated to students depending upon the workload assigned to the class.

5.3. Removal of Network access

1) The eligibility of network access holders is reviewed periodically. Access for individuals who no longer meet the eligibility criteria will be stopped.
2) The eligibility of network access is stopped to all people who use UTAB internet network to access illegal website resources.
3) Student network access is removed when the student is no longer enrolled.

5.4. Appropriate use of UTAB network resources

In support of academic instruction, research, public service, and administrative functions, UTAB encourages the use of, and provides access to, information technologies and network resources. This enables UTAB users to access global information resources, as well as the ability to communicate with other users worldwide. In keeping with its role and values, UTAB supports

the use of electronic communication for the conduct of official UTAB business and for individual professional purposes related to the UTAB's vision and mission.

1) Any computer or network device connected to the UTAB network shall be protected by antivirus software from malicious electronic intrusion. This rule applies to all devices connected, by any means, to the UTAB network including those owned by UTAB, private individuals such as the UTAB staff and students as well as partners.
2) UTAB computer users are individually responsible for the antivirus software and applicable operating system and software patches for devices under their control.
3) UTAB reserves the right to review any device attached to the network (public or non-public) for adequate virus protection.
4) UTAB reserves the right to deny access to the network to any device found to be inadequately protected.
5) Network access may be restored when the device has been cleaned and current antivirus software and applicable operating system and application patches have been installed.

Done at Byumba on 01 March 2016

Prepared by:	**Approved by:**
RUKUNDO Jean Premier Bienvenu	Prof. Dr. Ashraph Sulaiman
ICT Manager	Deputy Vice Chancellor – Academics & Research