BITS College

Office of ICT Support

ICT Policy

Revised July 2024

Addis Ababa

Table of Contents

1. INTRODUCTION

ICT (Information and Communication Technology) refers to technology that is used for the creation, processing, and distribution of data and information using any computing equipment and software, telecommunications, and digital electronics.

The College set out this ICT policy as an underlying guideline for proper, efficient, and effective use of ICT to succeed in achieving its mission and objectives. Therefore, this ICT policy document articulates policy guidelines and framework as program of actions for implementation and use of ICT.

The document is organized as follows. Section 2 outlines the purpose of the policy, ICT governance, and definition of important terms. Sections 3 to 15 present policy statements. Finally, Section 16 outlines the procedure for the amendment of the document.

2. GENERAL CONTEXT

BITS College encourages the use of ICT to share information and knowledge in support of its mission and activities. To this end, the Office of ICT Support Services shall implement, introduce, support, and provide ICT services and facilities in the College.

2.1 Definitions

In this document;

- E-learning is ICT-enabled transfer of skills and knowledge. It comprises all forms of electronically supported learning and teaching.
- "ICT" refers to any existing or upcoming technology that is used for the generation, processing and distribution of data and information using computer hardware and software, network, telecommunications, and digital electronics.
- "Users" refers to academic and administrative staff (permanent as well as contractual employees), currently enrolled postgraduate and undergraduate students (regular, in-service, and extension), offices (academic and and Administrative units), visiting scholars and guests, and other affiliated individuals or organizations authorized by the Dean of the College.
- "Office of ICT Support Services" refers to the Information and Communication Technology Support Services Office of the College.
- "System Administrator" refers to a person who is authorized as being responsible for the configuration, maintenance, and operation of the College Network.

- Software refers to the collection of programs installed on College servers or computers as well as on network devices such as switches and routers. The software could be locally developed by College staff, local vendors or purchased off the shelf.
- Software acquisition refers to the procurement of software that will be used for solving specific problems or improving the day-to-day activities such as administration, student management, teaching-learning, research, etc. of the College.

2.2 Purpose of the Policy

This policy has been established to:

i. provide guidelines for the conditions of acceptable and appropriate use of ICT resources installed and configured for use in the College,
ii. provide standards for users in the management and use of ICT resources,
iii. prevent/protect the system from attack, abuse, damage, loss or theft and for assuring the confidentiality, integrity and availability of data and ICT resources within the College,
iv. provide guidelines of detailed mechanisms for responding to external complaints about actual or perceived abuses originating from ICT resources in the College,
v. encourage and create awareness so as to enable users to understand their own responsibility for protecting ICT resources of the College, and
vi. provide guidance in the development, use and maintenance of a reliable, secure and cost effective ICT infrastructure that conforms to recognized standards for the access of internal and external information and learning materials in line with the objectives of the College.

2.3ICT Governance

ICT services in the College shall be managed by the Office of the ICT support services

The EMB of the Collegeoversees and advises ICT development and use in the College.

2.4.2 Office of ICT Support Services

In relation to this Policy, the Office of ICT Support Services is responsible for:

- the implementation of ICT policies, strategies and standards,
- the management of the network
- the management of the College's e-mail system,

- Internet access,
- the development, implementation and support of network systems and technologies including adequate connectivity and high speed network for data, voice and video,
- providing support to Offices of the Collegein determining the type of connection needed to link the computing equipment and labs to the College backbone,
- technical support of the College website, and
- providing user support services.

3. IT EQUIPMENT ACQUISITION, INSTALLATION, AND MAINTENANCE

3.1 Introduction

IT equipment refers to computers, computer peripherals, printers, photocopy and fax machines, scanners, hubs, switches, routers, servers, networking cables, etc. The purpose of this Equipment Acquisition, Installation,and Maintenance Policy is to provide procedures and guidance for the proper acquisition, installation,and maintenance of IT equipment.

Users shall follow thisIT equipment acquisition, installation, and maintenance policy.

3.2 Policy Statements

3.2.1 Acquisition

i. All purchases of new IT equipment or new components for existing IT systems must be made in accordance with organizational policies through a structured evaluation process. Such purchase requests shall be based upon a User Requirements Specification document and shall take account of long-term organizational business needs.
ii. Request for Proposals (RFP), Request for Information (RFI), or Invitations to BID (ITB) shall be issued by the responsible unit for purchasing but shall be reviewed by the appropriate Office of ICT Support Services before the release of the documents.
iii. Whenever possible, pooling the needs and requisition of all sections of the College to allow for bulk purchasing at economic rates shall be pursued.
iv. All IT equipment to be purchased shall fulfill the minimum standards such as integration, security, environmental friendliness, and further expandability as set by the College from time to time.

v. Prior to purchasing any hardware/equipment, a hardware acquisition form, which is reviewed by the appropriate Office of ICT Support Services, shall be submitted together with a purchase order to initiate the review process.

vi. The College shall maintain established standard configurations for all computers and IT equipment procured by the College. These equipment shall be procured with standardized hardware and software configurations as determined jointly by the appropriate Office of ICT Support Services and the Purchasing Department.

vii. The College shall systematically modernize its stock of computers to meet the demands of latest software, web access, and other basic tasks of computation and communication.

viii. Grants which are written on behalf of the College which require the purchase of computers/equipment shall adhere to this policy.

3.2.2 Installation

i. Only personnel authorized by the College shall install and configure IT equipment that belong to the College after consulting the installation guide and manual of the respective equipment. Such personnel are responsible for the safety of the devices they install.

ii. All new IT hardware installations shall be planned formally and notified to all interested parties ahead of the proposed installation date.

iii. All configured and installed IT equipment must be fully and comprehensively tested and formally accepted by users before being transferred to live environment.

iv. Computers, workstations, laptops, PDAs, and smart phones or other removable storage devices such as USB drives or memory sticks may be connected to the College network subject to the regulations of acceptable use as set out by the Office of ICT Support Services from time to time.

3.2.3 Maintenance

i. Adequate resources shall be made available for a regular maintenance of IT equipment.

ii. The College shall put in place an elaborate programme of refurbishment and replacement of obsolete and outdated computer equipment.

iii. All IT equipment owned, leased or licensed by the College shall be supported by appropriate maintenance facilities by qualified technicians.

iv. Deliberate or accidental damage to the College's IT property shall be reported to the officer in charge of IT security as soon as it is noticed.

4. SOFTWARE ACQUISITION, INSTALLATION, AND MAINTENANCE

4.1 Introduction

The purpose of this College Software Acquisition, Installation, and Maintenance Policy is to provide procedures and guidance for the proper acquisition, installation, and maintenance of software.

Users shall follow this software acquisition, installation, and maintenance policy.

4.2 Policy Statements

4.2.1 Acquisition

i. All requests for a new application system or software enhancements must be presented to the ICT support Service with the user requirements presented in a User Requirements Specification document.

ii. Request for Proposals (RFP), Request for Information (RFI), or Invitations to BID (ITB) shall be issued by the responsible College unit for purchasing but shall be reviewed by the appropriate Office of ICT Support Services before the release of the documents.

iii. Any purchase of software that necessitates data interface with any College enterprise application must be approved by the Office of ICT Support Services.

iv. All software packages running on the College's infrastructure must be compatible with the College's preferred and approved computer operating system and platform as set by the Office of ICT Support Services from time to time.

v. With exceptions of software that are used in teaching-learning which are mostly open source, The College shall use only licensed software and the terms and conditions of all End User License Agreements shall be strictly adhered to.

vi. All software associated with the College and which are not in the public domain, shall be treated in accordance with any applicable copyright agreements and restrictions. Such materials shall be licensed (if required) in an appropriate manner and shall be obtained only in a legal manner from a legal source.

vii. Patches to resolve software bugs shall only be applied where verified as necessary and by the appropriate Office of ICT Support Services. They shall be from a reputable source and shall be thoroughly tested before use.

4.2.2 Installation

i. The installation of new or upgraded software shall be carefully planned and managed, ensuring that the increased IT security risks associated with such

projects are mitigated using a combination of procedural and technical control techniques.

ii. Upgrades to software shall be properly tested by qualified personnel before they are used in a live environment.

iii. The decision whether to upgrade software shall only be taken after the consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and the necessity for such a change.

iv. Necessary upgrades to the Operating System of any of the College's computer systems shall have the associated risks identified and be carefully planned, incorporating tested fall-back procedures.

4.2.3Maintenance/Support

i. Software maintenance/support shall be based on the support level agreed upon as part of the purchase approval process.

ii. All application software shall be provided with the appropriate level of technical support by ensuring that any software problems are handled efficiently with their resolution available in an acceptable time so as to ensure that the College's activity is not compromised.

iii. Software faults shall be formally recorded and reported to those responsible for software support/maintenance.

5. INTERNET

5.1 Introduction

Internet is one of the major services on the College. The College provides Internet services on its network to support its academic and administrative functions to users.

For proper usage of Internet services, users are required to firmly follow this Internet policy.

5.2 Policy Statements

i. Access to the Internet shall be available to all eligible users.

ii. Internet use in the College is for the purpose of conducting the College's business only.

iii. Limited personal use of the Internet is acceptable, provided such personal use does not interfere in any way with the College business use of the facilities and does not jeopardize the operation of the College's computing facilities.

iv. College facilities may under no circumstances be used to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related Internet sites.

v. The creation, dissemination, storage and display of obscene or pornographic materials, indecent images of children, hate literature, defamatory materials or materials likely to cause offence to others is prohibited.

vi. The College's Internet facility shall not be used to setup e-business activities not related to the College.

vii. The use of the College's Internet services to engage in hacking other sites, and accessing unauthorized information within and outside the College are not allowed.

viii. Any user who will utilize the Internet service shall use the proxy service provided. If there is any need for direct access to the Internet, the user shall provide a formal letter from his/her respective academic unit or office and get the approval of the responsible organ of the College.

ix. A firewall shall be used on College network to control all data packets and connection requests; only explicitly permitted traffic is allowed through the firewall, all other traffic shall be rejected; all traffic passing through the firewall must be capable of being logged and audited; packet filtering shall be used with rules, which keep the risk to a minimum.

x. Where possible, access by outside users (e.g., using modems) shall be restricted.

xi. The downloading, storage and dissemination of copyrighted materials including software and all forms of electronic data without the permission of the copyright holder or under the terms of the licenses held by the College is prohibited.

6. ELECTRONIC MAIL (E-MAIL)

6.1 Introduction

E-mail service is one of the major services of the College. Hence, the College provides e-mail services on its network to support its academic and administrative functions to all users. In order to enable users share information, improve communication, exchange ideas and improve productivity, the College encourages the use of e-mail.

Access to e-mail services and facilities at the College is a privilege and must be treated as such by all users. Abuse of these privileges can be a matter of legal action or official College disciplinary procedures.

For proper usage of the e-mail service, users are required to firmly follow this e-mail policy.

6.2 Policy Statements

6.2.1 E-mail Use

i. E-mail service shall be made available to all College Staff

ii. User requests for an e-mail account shall be directed to their respective academic or administrative units.

iii. Academic and administrative units may request e-mail accounts for visiting scholars and other guests who are in some way affiliated with the College. The respective academic or administrative unit shall notify the responsible body when relationship of the account holder with the College no longer exists.

iv. E-mail use in College is for the purpose of conducting the College's business only and may not be used to send "for-profit" messages.

v. The College allows the limited personal use of the e-mail system, provided that such personal use does not interfere in any way with the College's business use of the system and does not jeopardize the operation of the College's computing or e-mail facilities. Only responsible personal use is permitted provided that it is not likely to cause loss to the College, is not for personal financial gain, does not contravene any of the College's policies and guidelines, is not detrimental to the College's image, and does not interfere with work.

vi. Pornography, or sending pornographic jokes or stories via e-mail, is considered sexual harassment and will be addressed per the disciplinary measures policy of the College.

vii. Use of the e-mail system to engage in communications that are in violation of the College policy including but not limited to transmission of abusive, obscene, offensive or harassing messages, or messages that disclose personal information without authorization is prohibited.

viii. Attempts to falsify identity, or to pretend of having a different affiliation with the College when sending e-mail from the College computer as well as conduct of any social engineering is prohibited.

ix. E-mail service shall not be used for junk or unsolicited bulk mail, and chain letters.

x. Using the identity and password of someone else for access or otherwise attempting to evade, disable, or "crack" password or other security provisions is not allowed.

xi. Users are responsible for all e-mail originating from their User ID.

6.2.2 Security and Confidentiality

i. The contents of e-mail messages sent or received are generally intended to be confidential.

ii. A user's e-mail address may be included in the College's Phonebook Database so that people from anywhere can look up a user's e-mail address based upon knowledge of a full name.

iii. A user's e-mail received/sent through the College is considered private. The College shall not read the content of an e-mail unless there is a court order

iv. The College reserves the right to refuse e-mail from outside hosts that send unsolicited (bulk), mass or commercial messages, or messages that are considered as threats, or messages that appear to contain viruses, and to filter, refuse or discard such messages.

6.2.3 Closure of an e-mail Account

i. A user's account of a staff member that is dismissed, has resigned, retired or died shall be closed/deactivated with immediate effect when the event is notified to the Office by the responsible body. The associated data with the closed account shall be archived for one semester.

ii. A user's account of a student that is dismissed or has graduated shall be closed/deactivated with immediate effect when the event is notified to the Office by the Registrar. The associated data with the closed account shall be archived for one semester.

iii. Anyone who does not comply with the rules and regulations of the College's e-mail use may have his/her account closed/deactivated with immediate effect.

iv. If the employee is found to have breached the email policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

6.2.4 User Naming

This shall be done as per the College's rules and procedures.

6.2.5 Disk Space Quotas

This shall be done as per the College's rules and procedures.

7. WEB PUBLISHING

7.1 Introduction

The College provides Web publishing services to support its academic and administrative functions. The College's Website is an official publication of the College. Its mission is to promote the College and provide accurate and up-to-date information in an accessible and attractive manner to audiences inside and outside of the College. It is an all-encompassing site and a virtual reflection of the College community and its heritage.

The Website is an invaluable tool that offers new opportunities for communicating information about the College to a worldwide audience. It is expected to represent the College's mission and its character.

The College Web service supports official, academic, and unofficial pages.

- Official pages are those of College offices such as academic units, Library, registrar and administrative units. They represent the College and its offices to the College's various audiences: potential students, currently registered students, employees, donors, and visitors. Official pages must conform to the design styles adopted by the responsible office to give the site unity, coherence, functionality and readability.
- Academic pages are those pages used for course delivery or instruction. These include pages created by instructors for courses and by students in order to fulfill course requirements.
- Unofficial pages are the remaining College mission related pages. They are the home pages of staff, faculty, and student personal pages. In addition, organizations that are affiliated with or support the College, but not directly a part of the College shall also have space for Web pages. These include all student clubs, Alumni Association, donors and partners of the College. However, space on this resource is a privilege, and all users are expected to follow the established Website policy.

Because of its importance in building the College's future and a means for communicating with the public, this policy is set to govern the nature, content, format, maintenance, timeliness and ownership of information contained on the official and unofficial pages of the College Website.

7.2 Policy Statements

7.2.1 Official College Web Pages

i. The contents of all official pages must reside on the College's Web server.

ii. All official pages shall be built using template pages supplied through the Web administrator and shall be maintained and regularly updated by the responsible College offices or academic units.

iii. Each official page within the College's Website shall be readily identifiable as a part of its site by the use of the College logo or logotype, a specific palette of colors and specific typefaces.

iv. Each official page shall carry the e-mail address of the academic unit or office responsible for its upkeep.

v. Official pages shall be accurate, well-written, concise, and free of spelling and grammatical errors.

vi. Academic units shall carry navigational links to each of its faculty member's home pages or to the e-mail addresses and telephone numbers of those faculty members who choose not to have a home page.

vii. All official pages shall be regularly monitored by the Web administrator to ascertain that the material is current. Those with outdated materials will be notified to update their page or remove the outdated material.

viii. Graphic elements and photographs on official pages shall be governed by the College's rules and procedures.

ix. Interactive features shall not be used on the Website's official pages without prior approval from the Web administrator and a plan for periodically updating the material contained in them.

7.2.2 Unofficial Web Pages

i. All unofficial Web pages shall carry navigational links to the College's home page, the author's name, and how to contact (either an e-mail address, a telephone number, or both) and the most recent date of the page's modification.

ii. Unofficial pages shall be governed by all applicable policies of the College, for example, College policies concerning sexual harassment and hate crimes/incidents.

iii. Unofficial Web pages may not be used for commercial uses, sales or money-making ventures except those authorized by the College administration.

iv. Any unofficial page on the College site that violates College policies may be removed from the Website immediately by the Web administrator in consultation with the Office of ICT Support Services.

v. In order to be given the privilege of a personal page, the author shall sign a form agreeing to comply with the College's Website policy.

vi. A disclaimer must appear on a personal Web page which reads:

> "The views and opinions expressed on these unofficial/personal pages on the College are strictly those of the authors. The contents of these pages have not been reviewed or approved by the College."

7.2.3 Web Authoring

i. All Web authoring tools shall be in compliance with the Content Management System used by the College.

ii. Web developers shall be provided with consultation and training, appropriate software, hardware, as well as individual assistance in the use of content management systems, mastering software and style for the Website.

iii. Web developers may choose from a selection of official College templates, colors and photos for composing pages representing their respective office(s). These shall be stored in a Website library maintained by the Office of ICT Support Services.

7.2.4 Website Security

i. A system of permissions shall be adopted and used to protect the security of the College Website.

ii. Those with full permissions to administer the site will be limited and will be designated by the Office of ICT Support Services as necessary to maintain websites.

iii. Permissions for Web developers will be limited to their areas of responsibility on the Website. Permissions to author on the site will be given by the Web administrator.

iv. All employees with full or limited permissions to the College Website are responsible for taking all reasonable precautions to protect both the public and developmental Website areas from vandalism, hacking and accidental alteration. This includes not sharing computer account information or passwords with others at the College and carefully monitoring access to personal computers in shared work areas.

7.2.6 Acceptable Use

i. Users are responsible for the Web pages that they publish under applicable College rules and regulations. Complaints alleging misuse of the Web service shall be directed to bodies responsible for taking appropriate disciplinary action. This may include the withdrawal of access to Web service and other computing facilities.

ii. Without specific authorization by concerned bodies, the Web service may not be used for the following:

- Commercial advertising – this does not include advertisements related to or supporting the teaching, research, or service mission of the College, such as academic conferences, or listing of sponsors for a performance or special event.
- Publishing of Web pages of non-authorized users (such as non-College persons, organizations, etc.).
- Activities that would provide non-College-related personal financial/monetary gain.
- Alteration of pages of other users.
- Posting harmful, threatening, abusive, harassing, hateful or objectionable pages, or pages that violate any applicable regional, federal or international laws.

iii. Web pages are subject to periodic review and approval by the concerned Web master(s). The College reserves the right to remove any page that is in violation

of rules and regulations, is in conflict with the College's interests or is detrimental to the performance of its computing or network services.

7.2.7 Server Side Scripts and Domain Names

This shall be done as per the College's rules and procedures.

7.2.8 Supervision, coordination, development, and maintenance of pages

This shall be done as per the College's rules and procedures.

8. DOMAIN NAME SERVICES

8.1 Introduction

DNS is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. The purpose of this Domain Name Services policy is to provide procedures and guidance for the proper use of English-like domain names instead of IP address numbers for ease of access of a website.

8.2 Policy Statements

i. All domain name services of the College shall be managed and monitored centrally by the Office of ICT Support Services.
ii. A domain name request form shall be filled by College units requiring Domain Names.
iii. According to the College's DNS standards, all services that are provided by members of the College community as part of their official functions, and as part of the mission of the institution, shall be registered within the "mksaddis.com" domain.
iv. Domain names outside **bitscollege.edu.et** shall not be allowed on the College network. In exceptional circumstances, the approval of the President of the College or a designated body is required.

9. E-LEARNING

9.1 Introduction

9.2 Policy Statements

i. It is the College's Policy to promote e-learning and to integrate ICT in teaching and learning to enhance staff effectiveness thereby improving the quality of graduates and also provide greater access to education.

ii. The College shall ensure and require that all students and academic staff are trained on a continuous basis to equip them with the requisite skills to fully exploit the E-learning system developed for the various disciplines.

iii. It is in the College's interest that academic and research staff collaborate and form global e-learning networks with other academic and research interest groups.

iv. The College shall establish the appropriate common e-learning platform responsive to academic needs.

v. It is in the College's interest to provide greater access to College education through the development of ICT-based distance education.

vi. The College shall create and manage digital collections of academic resources and design digital library systems to support the teaching-learning process.

10. SECURITY AND SAFETY

10.1 Introduction

Security and safety is about protection of ICT infrastructure, data and the user community against attacks from internal or external sources. Relevant policies need to be put in place to ensure protection of users and ICT facilities like computer rooms, workstations, servers, switches, hubs, routers, firewalls, network wiring systems and other small or large ICT devices.

Deliberate attempts to degrade the performance of the College network or to deprive authorized personnel of resources or access to any College facilities is prohibited. Breach of security includes, but not limited to, the following: creating or propagating viruses, hacking, password grabbing, disc scavenging, social engineering, etc.

The College shall give high priority for preventing threats from being materialized and therefore users are required to adhere to the security and safety policy stated below.

10.2 Policy Statements

10.2.1 Physical Access

10.2.1.1 General

i. All College computer hardware shall be marked, either by branding or etching with the name of the College unit and name of the office or computer laboratory where the equipment is normally located.

ii. The College shall identify and isolate secured areas (such as server rooms) from physical contact or access. Secured areas shall be entered only by authorized personnel.

iii. All doors giving access to rooms or areas with computer equipment both from within and outside the building shall, as a minimum, be fitted with metal grills.

iv. All external windows to rooms containing computer equipment at ground floor level or otherwise visible to the public shall be fitted with window blinds or obscure filming.

v. Rooms and buildings incorporating high-density computer equipment shall have intruder detection alarm equipment or surveillance camera system installed or both. Where such facilities are not affordable, security personnel shall be used.

vi. During non-working hours, secure areas shall be protected against intrusion by appropriate access control, locks, and surveillance systems or by security personnel.

vii. The College shall put signs or sign board labeled as "Authorized Personnel only" in areas where there is physical access restriction.

viii. Visitors shall be allowed to enter secured areas only with the approval of an authorized administrator for clearly specified period and under the supervision of authorized Collegepersonnel.

ix. Visitors whose stay in the secured area is claimed important shall need approval from the highest official in the ICT administration or his/her delegate and shall have temporary ID.

x. Only authorized personnel are permitted to take computerized equipment belonging to the College off the premises and they are responsible for its security and safety.

10.2.1.2 Servers

i. All servers shall be kept securely under lock and key.

ii. Access to the system console and server disk or tape drives shall be restricted to authorized personnel only.

iii. Computer servers shall be housed in a room built and secured for the purpose.

iv. Computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

10.2.1.3 Workstations

i. Users shall log out of their workstations when they leave their workstation for any length of time.

ii. All users of workstations, personal computers or laptops shall ensure that their screens are locked when not being used.

iii. All unused workstations shall be switched off outside working hours.

10.2.1.4 Switches

i. LAN and WAN equipment such as switches, hubs, routers, and firewalls shall be kept in secured rooms. In addition, the equipment shall be stored in lockable communication cabinets.

ii. All communication cabinets shall be kept locked at all times and access shall be restricted to authorized personnel only.

iii. Whenever legitimate access to communication cabinets is necessary, it shall be done with physical supervision of the responsible personnel.

10.2.1.5 Wiring

i. All internal or external network wiring shall be fully documented using convenient means including positioning technologies like GPS.

ii. All unused network points shall be de-activated.

iii. All network cables shall be periodically scanned and readings recorded for future reference.

iv. Users shall not place or store any item on top of network cabling.

v. Redundant cabling schemes shall be used where possible.

10.2.1.6 Monitoring Software

i. The use of monitoring tools, such as network analyzers or similar software, shall be restricted to authorized personnel who are responsible for network management and security purpose only except when explicit permission is given for academic and research purposes by an authorized person.

ii. Purposefully scanning internal or external machines in an attempt to discover or exploit known computer software or network vulnerabilities is prohibited.

iii. Network monitoring tools shall be securely locked when not in use.

10.2.1.7 Electrical Security

i. Power feeds to servers and workstations shall be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.

ii. All switches, routers, firewalls and critical network equipment shall be fitted with UPS.

iii. Where possible, generator power shall be provided to help protect computer systems in the case of a mains power failure.

iv. All UPS equipment shall be tested periodically.

10.2.1.8 Inventory Management

i. The College shall keep a full inventory of all computer equipment and software in use throughout the College.

ii. Computer hardware and software audits shall be carried out periodically to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

10.2.2 Safety

i. The College shall set out procedures and operation manual with the consideration of preventing anticipated threats that may damage physical devices.

ii. The College facilities shall be adequately protected against fire, water and physical damage.

iii. No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.

iv. Only suitable and approved cleaning materials shall be used on IT equipment owned by the College.

10.2.3 Network Control

i. Connecting any computer device to the College network unless it meets the security standards established by the College is prohibited.

ii. Involving in pervasive computation for financial gain without the knowledge and explicit permission of the College is prohibited

iii. Permission shall be sought from the office for any third-party network connections to the Internet or any external networks.

iv. The setup of IT equipment for network access shall be done by the responsible office or under its direction.

v. The College network infrastructure shall be secured against e-mail spam, intruders or hackers, break-ins, viruses, Trojan horses, worms and other disruptive software.

10.2.4 Antivirus

i. The College shall install standard antivirus software to ensure that all servers, workstations, and notebooks owned by the College are protected against virus infection. Antivirus software(s) shall be updated on a regular basis.

ii. All computers used in the College must have the College's standard antivirus software installed. Every user shall avail computers in use for the installation of the antivirus software.

iii. Users shall call for assistance immediately if a virus incident is noticed and cannot be cleaned by the user.

iv. Deliberate actions that might reduce the effectiveness of any antivirus or other IT security management precautions installed by authorized Collegepersonnel is prohibited.

10.2.5 Transfer and Disposal of Computers and Software

i. Offices of the College shall work with the concerned Office of ICT Support Services to ensure that procedures consistent with security best practices are followed for the reliable removal of licensed software and confidential data before equipment transfer or disposal takes place.

ii. IT equipment owned by the College may only be disposed off by authorized personnel who have ensured that the relevant security risks have been mitigated.

iii. Disposal of devices shall not entail environmental damage or abuse and shall follow the disposal instruction manual of the respective hardware.

iv. All computers shall be fully formatted and restored to factory default before they are disposed off.

v. All such formatted computers shall then be disposed off according to the disposal procedures of the College.

vi. The disposal of software shall only take place when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.

10.2.6 User Responsibilities

i. Only eligible users shall be allowed to use the College's ICT facilities.

ii. The user community as a whole shall not use the facilities, software, services and systems in any illegal or otherwise unauthorized manner.

iii. Using computing resources (CPU time, disk space, bandwidth) in such a way that causes excessive strain on the computer systems or disrupts, denies or creates problems for other users shall not be exercised.

iv. The deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting the data belonging to other users is prohibited.

v. The College reserves the right to monitor and record all activities within the College when users access the facilities, software, services and systems.

vi. Users shall take all reasonable steps to ensure that computer equipment in their possession or under their control is protected at all times against theft and accidental or deliberate damage.

vii. Users issued with a username and password for the first time shall change the initial password immediately.

viii. Users shall not share the password with others and shall not write or keep the password in an insecure location.

ix. Use of user accounts or credentials without the consent of the legal holder of the credential is prohibited. Furthermore, users of systems will not divulge passwords, pins, private keys or similar elements to anyone else, and they will not exploit sessions left open or otherwise steal the "identity" of another user.

x. All user passwords shall be seriously treated as private and confidential and must not be exposed, shown or given to any party other than the user.

xi. Users shall change their passwords on regular basis. It is recommended to create a password based on combinations of numeric and alphabetic characters with a minimum length of 8 characters. It is not recommended to have a password that is the same as the username, recycled or previous passwords or a name which is associated with the user.

xii. Personal laptops connected to the network shall adhere to the following guidelines.

- Their operating system and any installed software shall be fully patched and kept up-to-date.
- Up-to-date antivirus software shall be installed to provide protection from viruses, worms, Trojan horses, disruptive programs or devices or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of the College.

10.2.7 Logical Access Control

i. Access to network facilities shall be through user IDs and passwords. Appropriate domain control mechanism shall be put in place for the purpose.

ii. All users shall have user account and access rights and privileges that shall be set accordingly.

iii. The College’s facilities shall not be used for anything that may bring the name of the College into disrepute or expose the College to the risk of civil action.

iv. Where applicable, all users shall not have the same access level to specific information or resource and access to certain systems and information therefore are determined at the time of issuance of an account based on the job role of the person.

v. Intentional creation, execution, forwarding or introduction of any viruses, worms, Trojan horses or software code designed to damage, self-replicate or hinder the performance of the College network is prohibited.

vi. Accounts on all systems shall be audited each semester for validity.

11. USER SUPPORT AND TRAINING

11.1 Introduction

A variety of services may be developed and produced in response to the business requirements of the College. Upon production, these services are distributed (or made available) to users. Thereafter, continuous and carefully tailored training and support is necessary in order for the users to fully exploit them. The objective of this policy is, therefore, to outline a guiding reference when providing user support and when planning for, organizing, and conducting ICT training.

Users and the service providing unit are required to adhere to the following policy on user support and training.

11.2 Policy Statements

11.2.1 User Support

i. User support shall be provided in the form of informed help on academic and administrative computing and information to all users.

ii. Computing services shall continue to be provided with strong user support to ensure integrated access to information services.

iii. All information system hardware faults shall be reported promptly and recorded in a hardware fault register.

iv. The ICT personnel of the College shall be the first point of call for user support.

v. Technical audits shall be undertaken at least every three years by the Office of ICT Support Services to determine the performance of computers and recommendations shall be made for replacement or otherwise.

11.2.2 ICT Literacy

i. It shall be mandatory for all Collegeprofessional staff to be literate users of ICT services, the level of literacy being in line with the demands of their job functions.

ii. Computer literacy programmers shall be offered to the College community with the objective of not only ensuring user satisfaction but also reducing the user support load on the involved ICT personnel.

iii. Training shall focus on building skills in users making them effective in exploiting provided ICT resources.

11.2.3 Training

i. ICT training targeting the College community shall be scheduled on a continuous basis.

ii. The College shall develop curricula for all training including development of source material.

iii. Where external training is sourced, the College shall jointly with the external training agency, customize the content to meet the training needs of the users.

3.15.2.4 Acknowledgement of Training

i. The College or an authorized external training agency shall issue certificates on successful completion of training and examination.

12. APPLICABILITY AND USE

12.1 Introduction

The services of the College are primarily meant to support the essential functions of teaching, research and administration of the College. The users of these services are essentially those that are engaged in these College activities. In order to ensure that the ICT resources are used in an effective and lawful manner, it is essential to precisely define the target users and the terms and conditions under which the ICT resources are used. The main objectives of this section of the College's ICT policy are the presentation of the detailed specifications of who the target users are and the terms and conditions of use of the ICT resources to ensure that the resources are used in an effective, efficient, ethical and lawful manner. The policies set out in this section have two components: the specification of the target users and the unacceptable activities in the use of ICT resources.

12.2 Policy Statements

12.2.1 Applicability

The following use policy shall apply to and govern

i. All College offices and hosted societies or research offices that make use of the ICT resources within the College.

ii. All ICT systems, equipment, connected locally or remotely to the College ICT infrastructure.

iii. All College owned and administered ICT resources including, but not limited to, servers, network devices (such as routers, switches, backup power supplies,

cablings both fiber and copper), personal computers, network equipment, operating systems and application software.

iv. All connections made to external networks through the College network.

v. All ICT related data, report and reports derived from the ICT facilities within the College.

vi. ICT projects, planned or in progress.

vii. The public other than users of the College may access information as set by the College via the official website.

12.2.2 Users

Users of the College infrastructure, facilities, and resources include academic and administrative staff (permanent as well as contractual employees), currently enrolled postgraduate and undergraduate students (regular, in-service, and extension), offices (Colleges, Faculties, Schools, Departments, Colleges, and Administrative units), visiting scholars and guests, and other affiliated individuals or organizations authorized by the President or his/her designate.

A user may be given access to all or a particular part of the College facilities, depending on individual work or study requirements.

12.2.3 Rights

Users have the right to use the College facilities to carry out legitimate activities. Users have also the right to privacy while engaged in legitimate activity. This right may on occasions be superseded as indicated in 12.2.4 below (Privacy).

12.2.4 Privacy

Users have legitimate expectation to privacy in the carrying out of approved activities.

In general the College does not monitor or restrict the content of material transported across the College. The College, however, has a legitimate right to inspect any data on a computer system on the College (regardless of data ownership), to prevent, detect or minimize unacceptable behavior on that computer system. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved. This section formalizes these principles.

i. The College, through the Office of ICT Support Services, may monitor or use any account, device, or terminal without notice.

ii. In the course of carrying out computer system auditing operations, the College may access and copy any file on any computer system owned by the College.

Subject to all other conditions of this policy, the College is obliged to maintain confidentiality of the data it acquired as a result of such access.

iii. The College is free to capture and inspect any data on any networking infrastructure owned by the College.

iv. The College has the right to give to any appropriate member of the College community, or law enforcement bodies, any information it possesses regarding the use of the College's resources.

v. The College may authorize specified personnel whose duties include monitoring the use of the College facilities to investigate the suspected security breaches or unauthorized access.

12.2.5 Violation

The consequences or penalty to follow as a result of non-compliance to the Policy or other regulation set forth in the Procedure Manual shall be adequately detailed in an unambiguous and concise manner in subsequent document(s) that may be produced during the implementation of this Policy.

Furthermore, any offence committed against this policy is subjected to penalty in accordance with the College's legislation and/or by the respective law of the Federal Democratic Republic of Ethiopia.

13. ADMINISTRATION

13.1 Introduction

Administration of the ICT resources and services at central, local, and personal level is one of the core functions of the Office of ICT Support Services. The central level relates to managing primarily the backbone network platform that includes the College server farms at both central and campus levels, cables and active network devices between campuses and within campuses between buildings. The Departmental or Campus computer labs and resources, including specialized software and equipment, are considered to be local and the College controls their respective access to the network and supports their proper administration. Staff members who have their own desktop or lap top computers are responsible for their equipment.

13.2 Policy Statements

13.2.1 Server Administration

i. The administrator of a server connected to the College network is responsible for the security of that system.

ii. The system administrator monitors, logs accesses, and keeps other system logs that could be useful in establishing the identities and actions of people, programs and processes that use the system.

iii. Units that operate publicly accessible computers (i.e., computer labs or information kiosks) connected to the College network must implement safeguards against network abuse.

iv. Data that are considered confidential must not be publicly accessible.Administrators of servers containing confidential data are responsible to reasonably secure these systems so as to reduce the threat to the College as a whole.

v. All servers that provide access to the College network or Internet services shall require user authentication for authorized access.

13.2.2 Internal Computer Lab Administration

i. All College units that own computer labs shall appoint officers designated as computer lab administrators, who shall be in charge of their labs.Heads of units shall formally inform the Office of ICT Support Services of the names and contact addresses of their computer lab administrators.

ii. Computer lab administrators shall be responsible for the day to day running of a computer lab, and shall be the point of contact for Office of ICT Support Services on all operational issues regarding the lab.

iii. Computer lab administrators shall be responsible for the security of their labs and the lab's impact on the College or any other network. They shall be responsible for overseeing adherence to the College ICT Policy.

iv. Computer lab administrators shall be responsible for control of access to their computer labs; they shall ensure that only legitimate users can gain access to lab resources.

v. The Office of ICT Support Services shall furnish records of all IP addresses and related configurations assigned to hosts in any computer lab. The lab administrator or any other person shall, at no time, change these configurations without prior notification to the Office of ICT Support Services.

vi. Any College unit that wishes to add an external connection to their lab whilst the lab is connected to the College shall provide a diagram and documentation of the proposed connection to the Office of ICT Support Services with adequate justification. The Office of ICT Support Services shall then study such proposals for relevance, review it for any security concerns, and shall approve before implementations are allowed to proceed.

vii. No computer lab shall replicate the core production services provided by the Office of ICT Support Services. These services shall include, but not limited to,

proxy services, e-mail services, web hosting, and FTP services. The Office of ICT Support Services shall, alone, manage these services and/or authorize other units to extend these services.

viii. The Office of ICT Support Services reserves the right to interrupt lab connections if such connections are viewed to impact negatively on the ICT infrastructure, or pose a security risk. For this purpose, lab administrators or their delegates shall be available for emergencies; otherwise actions shall be taken without their involvement.

14. SYSTEM AND CONFIGURATION CHANGE MANAGEMENT

14.1 Introduction

The College keeps a detailed recording and updating of information that describes its computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied and locations and network addresses of hardware devices. In order to avoid some very costly errors, the College shall ensure that all system configurations and changes are introduced in a controlled and coordinated manner

14.2 Policy Statements

i. All system and configuration changes made to major system units and infrastructures shall be recorded on the change management log.

15. STRATEGY OF IMPLEMENTATION

In order to achieve the goals and objectives of the ICT policy, the Office of ICT Support Services will steadfastly pursue the following broad strategies.

i. Design service network systems that allow users to communicate to each other and with public ICT facilities.

ii. Set up organizational structures for the Office of ICT Support Services and the define duties and responsibilities of
    a. the director of the Office of ICT Support Services,
    b. each service under the director, and
    c. each team under each service.

iii. Adopt methods and procedures to ensure that required ICT system(s) is/are developed, deployed, and configured for serving the various component of the College's governance structure; and follow-up and coordinate the proper and efficient utilization of ICT resources.

iv. Promote and facilitate the participation of users and communities in ICT development.

v. Support the development of ICT systems and programs that enhance the participation of women and the physically challenged.

vi. Conduct awareness creation and capacity building through specialized and result-oriented training.

vii. Establish public information gateways or portals to harness develop and integrate public information resources.

viii. Promote bilateral and multilateral cooperation with organizations involved in the development and promotion of ICT.

16. AMENDMENTS

This ICT policy shall, in general, be reviewed at least every two years. However, the office in charge of executing the policy may, from time to time, propose amendments that are necessary to enhance the objectives of this policy. Before the enactment of such amendments, the executing office shall provide opportunities to its major stakeholders to comment on the proposal. Members of the College community who wish to propose amendments may submit their proposed amendments to the executing office.

17. SUMMARY OF DUTIES OF THE ICT PERSONNEL OF THE COLLEGE

Equipment

- Configure and deploy new and refurbished workstations, laptops and peripheral equipment.
- Install, troubleshoot, repair, update and maintain workstations and laptops.
- Install, maintain, and troubleshoot printers/copiers as well as manage toner requests.
- Setup and support audio/visual equipment for presentations and trainings on and off site.
- Install and configure peripherals including scanners, external drives, monitors and other peripheral hardware.
- Removal/disposal of non-functional equipment

Software

- Provide software and system troubleshooting and support.
- Install, maintain, troubleshoot, and update operating systems and user applications.
- Proactively schedule software upgrades and patching.
- Assure that all software is licensed and keep record of licenses.
- Track license and support contracts to include notification of renewal timeframe to management.

Network

- Monitor network to ensure network functionality and availability to all system users.
- Install, maintain, troubleshoot, and repair cabled, wireless and other network infrastructure.
- Support existing/new server/s and administer access rights for all users in the office.

Security

- Maintain local and server based anti-virus software.
- Inform and train users and management in how to adhere to the ICT policy of the College
- In case of virus infection clean out affected equipment.

Users

- Ensure computer is set up prior to new hire start date and any related moves.
- Handle the relocation of computer equipment as a result of office or personnel changes.
- Setup new user accounts and email accounts

- Troubleshoot, and repair user accounts and email accounts, assist in resetting passwords. Systems Planning
- Participate in research and recommendation of improved infrastructure processes and technologies to include growth planning.
- Provide procurement assistance including, but not limited to, researching solutions, engaging with potential vendors, making recommendations for product purchases and evaluating bids.
- Test new equipment and applications and provide thorough feedback.

Management of Vendor Services

- Work directly with vendors to schedule repairs and maintenance.
- Request and evaluate services with vendors and service providers.
- Work with ISP and other outside vendors to ensure dependable operations.

Training

- Train new and current employees on computer software and ICT systems.
- Create materiel and presentations for trainings and reports.
- Assess user capacity and suggest trainings and areas in need of improvement.

Routine Administrative Tasks

- Create and maintain inventory, which may include hardware, software and various items such as laser printer cartridges and peripheral equipment.
- Maintain documentation of processes, procedures, and troubleshooting guides.
- Monitor and report ICT expenses.
- Assist with preparation of operating budgets based on estimated and actual expenditures for ICT systems and support needs.
- Keep ICT equipment, storage area and work area clean and organized.