UNIVERSITY FOR DEVELOPMENT STUDIES

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

November 2020

Table of Contents

Foreword

The vision of the University for Development Studies is "to be the home of world-class pro-poor scholarship". This is reflected in its motto "Knowledge for Service", as well as its Problem-Based Learning methodology of teaching, research, and outreach/internship. UDS seeks to achieve its vision by promoting an equitable socio-economic transformation of communities through practice-oriented, community-based, problem-solving, as well as gender-sensitive and interactive research, teaching, and learning activities.

The impetus to successfully implement our activities is to ensure that the University's Information and Communication Technology resources are utilised to create and facilitate a world-class atmosphere to deliver its mandate.

The joint effort of all and sundry to make this policy document available is heartily acknowledged.

All members (staff, students, contractors, and visitors) of the University Community shall endeavour to ensure the optimum and safe utilisation of ICT resources for themselves and others and positively contribute to our "zero-harm" vision of the workplace.

Thank you.

Prof Gabriel Ayum Teye
Vice-Chancellor

Acknowledgements

The University is grateful to the Information and Communication Technology (ICT) Committee and Directorate of ICT that initiated and developed this ICT Policy.

Appreciation goes to the Director of ICT, Dr. Abdul Wahid Mohammed, for developing the first draft of the Policy. Specific acknowledgement goes to the Committee members for developing and drafting this Policy: Prof. Francis Kweku Amagloh (Chairman), Mr. Stephen Minta (Secretary), Mr. Sulemana Mahamoud (Member), Ms. Miriam Linda Akeriwe (Member), Ing. Mubarick Issahaku (Member).

Write Up History

Version	Drafted by	Amendment History	Submitted To	Approved by	Date
1.0	Dr. Abdul-Wahid Mohammed	First Draft	UDS ICT Committee	ICT Committee	10/11/2020
1.1	Prof. Francis K. Amagloh led Committee	Second Draft	UDS ICT Committee	ICT Committee	1/04/2021

1.0 Introduction

The University for Development Studies (UDS) considers Information and Communication Technology (ICT) vital in delivering its mission and vision. This Policy provides the bedrock for strengthening digital literacy among staff, students, and other stakeholders.

UDS shall continue to invest in digital technologies that will enhance teaching, learning, research, administrative and outreach programmes.

The University shall exercise its right regarding ICT resources under relevant Ghanaian Laws: , Data Protection Act, 2012; Electronic Communications Act, 2008 (Act 775); and Electronic Transactions Act, 2008

Further, the University shall strive to protect its ICT resources against loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT resources or the maintenance of its ICT resources.

1.1 Purpose

This Policy addresses all ICT needs in furtherance of teaching, learning, research, administrative, and outreach services while protecting the University community against litigations and victimization.

1.2 Scope

This Policy covers all ICT resources owned and or operated by UDS and all employees, students, visitors, contractors, and other stakeholders engaged with the University or any person registered to attend short courses, seminars, or workshops.

ICT facilities include but are not limited to software (proprietary and licensed), telephones, mobile phones, email, servers, the Intranet, the Internet, e-Services, computers, printers, scanners, other associated equipment, and any connection to the UDS-owned network.

2.0 Teaching, Learning, and Research

The University shall develop and maintain an enabling digital environment that will support optimal teaching, learning, research, and community outreach programmes.

3.0 Administrative Processes

The University shall ensure the effectiveness of its operational and administrative functions that shall drive productivity. All staff and student information, financial transactions, and internal managerial communication shall be managed through an integrated enterprise resource management system.

The integrated enterprise resource management system shall comprise of:

- Administrative management Systems
- Library Management System
- Students Management System
- Teaching and Learning Management Systems
- Health and Safety Management Systems.

4.0 University Website

The University shall develop and maintain a responsive and functional website with the University's approved domain.

The website's content shall be authored by the University Relations in accordance with the guidelines for publication procedure of the University on the University's website.

5.0 Electronic Communication

All staff and students in service of the University and designated offices shall be assigned an institutional email address ending with the University's approved domain.

All correspondence related to University activities shall be through the institutional email address, and such emails shall be considered as official correspondence.

Intranet- and internet-based platforms shall be developed for intra-communication among stakeholders in the University.

Where there is a need for record-keeping, the Registrar or representative shall archive such documents.

6.0 Internet Use

The use is restricted to legitimate University purposes only. For students, this generally means academic coursework and research as approved by a supervisor. Staff usage shall depend on the nature of their work. Users are employees, students, contractors, visitors, and other stakeholders. The examples of prohibited and permitted usage of Internet service are the following:

- The University will not tolerate its Internet service to be used in a manner that is harassing, discriminatory, abusive, rude, insulting, threatening, obscene, or otherwise inappropriate.
- It is illegal to use the University's Internet service of the University to harass, menace, defame, libel, vilify, or discriminate against any other person within or beyond the University.
- Users may be individually liable if they aid and abet others who discriminate against, harass or vilify colleagues or any public member. Users who adversely affect the reputation of another person may be sued for defamation by that aggrieved person.
- Users must not use the University's Internet service to collect, use, or disclose personal information in ways that are contrary to the university rules and regulations.
- Users must respect and protect the privacy of others.
- Users are forbidden to use internet service to access, store, or transmit pornographic material of any sort other than with specific written approval from the Registrar.
- The University forbids the use of internet service in a manner that constitutes an infringement of copyright.
- The Internet service must not be used to cause embarrassment or loss of reputation to the University.
- The University does not permit its Internet service for unauthorised profit-making or commercial activities and any personal gain.

7.0 Social Media

The University shall have official social media platforms (Facebook, Twitter, YouTube, Instagram, etc.). These platforms would use official marks to interact and communicate with a range of stakeholder groups, including prospective and current students, staff, alumni, donors, and research collaborators to be managed by the University Relations Office.

Use of the University's name, logo, and other marks on social media without permission is illegal. Persons or entities interested in using the University's trademarks (name, logo, etc.) shall seek permission from the Registrar. The use of the University's trademarks must comply with the University regulations.

8.0 Media Recording and Surveillance

The University recognizes and supports the application of ICT in maintaining the safety and security of staff, students, and its properties:

- Video and audio surveillance equipment shall be installed at strategic points of UDS-owned facilities except where staff and students have a reasonable expectation of privacy.
- Notification of the operation of surveillance equipment shall be made accordingly.
- Recording by staff and students for academic and administrative purposes shall adhere to the University's regulation.
- There shall be no media recording without the knowledge and consent of the parties involved unless authorised by the University.
- The University supports the use of video/audio surveillance equipment. The contents of video/audio must comply with relevant policies.

9.0 ICT Resource Management

The Directorate of ICT through the ICT Committee shall report on the operations and maintenance of the ICT resources to the University Management and the University Council.

10.0 Roles and Responsibilities

The Directorate of ICT shall:

- Be responsible and accountable for all aspects of the design, implementation, administration, and maintenance of all ICT security systems and the processes and procedures by which these operate. It must immediately suspend privilege, access, and services to any user in breach of this Policy pending further inquiry. Such restrictions as applied are subject to review by the ICT Committee of the University.

- Account for all ICTs and information resources in their area of jurisdiction that is connected to campus networks.
- Provide and maintain a database of unique identifiers for all network-connected ICT assets.

- Assess the security risk of all ICT systems and apply such security systems and processes as are consistent with the mitigation of this risk.

- Provide or commission the physical security of all enterprise servers, databases, backbone network switches, and ICT management, teaching, and learning platforms.

- Procure, implement, and maintain the logical security systems necessary to protect University electronic data and information assets from misuse, damage, loss, or unauthorised access.

- Develop, document, and publish the ICT security guidelines following informed best practice.

- Promote a security awareness campaign for users of University ICT systems and collaborate with functional departments to design and deliver end-user ICT security awareness training.

- Present an audit report on Service Level Agreement at all regular ICT Committee meetings of the University.

Heads of Departments/Units/Sections with functional ownership of data and information resources shall:

- Determine the levels of authority in terms of access to the Departments/Units/Sections systems.
- Ensure every user in their jurisdiction and span of control is informed of the security requirements

Users of the services are responsible for maintaining the security of their interfaces to University-owned ICT data, and information resources by complying with University policies and regulations and related national and international laws. Persons found to violate this Policy may be liable to disciplinary action under University regulations. Violation may also constitute a breach of national law.

11.0 Monitoring

The ICT Committee through the Directorate of ICT shall monitor the University's ICT resources and ensure the following:

- Users must not download or store copyright material, post copyright material to the University's website, transfer copyright material to others or burn copyright material to CD ROMs or other storage devices using ICT resources unless the copyrighted material is appropriately licensed. Copyright material includes software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s), and video files.
- Users must not use the ICT resources in inappropriate ways, which are likely to corrupt, damage, or destroy data, software, or hardware, either belonging to the University or elsewhere, whether inside or outside the network (**Note:** This does not apply to specially authorised University's ICT staff who may be required to secure, remove or delete data

and software, and dispose of obsolete or redundant ICT resources as part of their ICT resource management duties.

- Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to any ICT resource unless authorized to do so. All faults or suspected faults must be reported to the ICT Help Desk.

- ICT resources must not be used to distribute unsolicited advertising material from organisations having no connection with the University or involvement in their activities.

- University email lists generated for formal University communications must not be used for any other business.

- Files may only be accessed or downloaded if they are work or study-related. In any case, files may only be downloaded if it is legal to do so, and steps have been taken to ensure that the files are free from viruses and other destructive codes.

- Files can only be attached to email messages if they are free from viruses, malicious, or other destructive code.

- Users must not attempt to gain unauthorised access to any ICT services. The use of another person's login, password credential is not permitted. Users shall not exploit any vulnerabilities in the systems (except authorised staff when checking systems' security as part of their duties) or use any technology designed to locate such vulnerabilities or circumvent security systems.

- Users must not facilitate or permit the use of the University's ICT resources by persons not authorised by the University.

12.0 Procurement and auctioning of ICT Resources

Procurement and auctioning of ICT resources shall be in accordance with the provision of this Policy and in accordance with the Public Procurement Act 663 of the Republic of Ghana.

13.0 Disposal of ICT Resources

Disposal of ICT resources shall be in accordance with the provision of this Policy and in accordance with the Hazardous and Electronic Waste Control and Management Act 917 of the Republic of Ghana.

14.0 Orientation and Policy Dissemination

As a new policy, workshops shall be organised by the Directorate of ICT with the support of the Registry for all staff members and students. Subsequently, newly employed staff should be given education on the ICT guidelines developed by the Directorate of ICT. Links to an electronic copy of the Policy shall be available on the University website.

15.0 Audit, Monitoring, and Review

The ICT Committee is responsible for monitoring the effectiveness of this Policy.

- The Committee shall receive an annual review from the Directorate of ICT at a workshop to prepare the annual report to be submitted to the Council.
- This Policy shall be reviewed after the first year of ratification by the Academic Board. Subsequently, reviews shall be done every five years or sooner as determined by the Academic Board.

16.0 Statement of Liability

The University shall not be liable for any infringement, violations, errors, omissions, loss or damage claimed or incurred due to any use of UDS ICT resources without fully complying with this Policy manual's tenets. Such users take full responsibility for the actions therein.

References

[1] M. Kulpa and K. Johnson, "Sample Policy," *Interpreting the CMMI (R)*, vol. 113. pp. 371–372, 2003, doi: 10.1201/9780203504611.axl.

[2] Government of Ghana, "Hazardous and Electronic Waste Control and Mgt Act 917.pdf." pp. 1–41, 2016.

[3] Great Lakes University, *Great Lakes University of Kisumu ICT Policy*. 2016, pp. 1–22.

[4] M. University, *Mzuzu University ICT Policy*, vol. 3. 2008, pp. 1–3.

[5] Kibabii University College, *Information and Communication Technology (ICT) Policy*, no. March. 2014, pp. 1–15.

[6] Kwame Nkrumah University of Science and Technology, *Policy for Development and Use of Open Kwame Nkrumah University of Science and Technology*, August. 2010.

[7] University of Ghana, "Email Policy | University of Ghana Computing Systems." [Online]. Available: https://www.ugcs.ug.edu.gh/policies/email-policy. [Accessed: 27-Nov-2020].

[8] University for Development Studies, *University for Development Studies Statutes*. .

[9] Government of Ghana, "Public Procurement Act 663." pp. 1–93, 2003.