DAMBAI COLLEGE OF EDUCATION

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

DACE/ICTP001/2020

TABLE OF CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

DACE/ICTP001/2020

1. INTRODUCTION

The National Policy on Education and the emergence of the information age has brought to the fore the important role that information, knowledge, and technology play in facilitating socio-economic development.

The effective use of information, technology and knowledge is becoming the most critical factor for rapid economic growth and wealth creation as well as improving the socio-economic well-being of people.

Advances in digital technology and ICT have led to an increased interest in considering potential applications of ICT in education and has sparked intense interest and experimentation in teaching and learning.

The initiative of ICT Policy in the College is inspired by the tremendous potential of ICT for enhancing outreach and improving quality of education. This policy seeks to provide guidelines to assist the College in optimising the use of ICT in teacher education.

2. THE POLICY STATEMENT

The mandate of the College is to train competent teachers through quality teaching and learning, research, and service to the Ghanaian and global society. As the Basic school curriculum evolves to become more ICT inclined the college aims at training teachers who will be skilled in using ICT to support teaching, learning and research across the curriculum. To achieve these, the College is committed to developing a robust ICT system that will facilitate education within the College community and promote e-learning and e-education as well as life-long learning among staff, student teachers and other stakeholders.This policy therefore seeks to provide guidelines for the actualisation of this vision.

3. PURPOSE/OBJECTIVES

The purpose of this policy is to:

a. educate staff, student teachers and the wider community on acceptable standards in using the College's ICT resources effectively as a tool for teaching, learning and research.

b. specify the responsibilities and required behaviours of users of the College's Management Information Systems (MIS), networks and computers.

c. support and develop lifelong learning of staff, student teachers and the wider community.

d. integrate ICT in teaching and learning and improve leadership in the College.

e. outline the acceptable use of ICT resources in the College.

The policy objectives are to:

i. provide optimum security for the use of the College's Management Information System (MIS), networks and computers.

ii. provide opportunities and expertise that will allow users of ICT in the College to access a range of Information and Communication Technology resources.

iii. support the sustainable integration of ICT tools towards improvement of governance, inclusivity and gender responsive management practices.

iv. ensure tutors are equipped with ICT knowledge and skills to undertake research work and support student teachers' ICT skill development.

v. strengthen ICT pedagogy in the College by promoting tutor awareness and positive attitude toward ICT usage.

4. SCOPE OF THE POLICY

The policy applies to College staff, student teachers and any other persons, who may be granted permission to use the College information and communication technology facilities.

5. SUPPORTING PROCEDURES

A. ICT TRAINING

i. The College shall be committed to providing training for all users of new systems to ensure that the use of the system is both efficient and does not compromise information security.

ii. The training of individuals in ICT shall be mandatory; with any technical training being appropriate to the responsibility of the user's job function. When staff change jobs, their ICT needs must be re-assessed and any new training shall be provided as a priority.

iii. All new staff shall receive mandatory ICT awareness in terms of training as part of their induction.

B. ICT LITERACY AND COMPETENCY ENHANCEMENT

i. The ICT literacy programme shall provide a broad set of generic skills and conceptual knowledge to staff and student teachers.

ii. The ICT literacy programme shall not focus on mastering the use of specific software applications.

iii. Acquisition of ICT knowledge and skills in the College shall go through the following stages, which shall be revised periodically to keep pace with changing technology.

Stage 1: Basic: Student teachers and staff shall be made to acquire basic knowledge and skills on: computing and other ICT tools; techniques in ICT operations, storage, information retrieval and data management, use a computer to achieve basic word and data processing tasks; connect, disconnect and troubleshoot basic storage, input and output devices connected to the internet, use e-mail and web surfing, use search engines.

Stage 2: Intermediate: Student teachers, staff and other stakeholders shall be trained to acquire basic knowledge and skills on creation and management of content using varieties of application software and digital devices; using websites and search engines to locate, retrieve and manage content, tools and resources; install, uninstall and troubleshoot simple software applications for the award of certificate in ICT proficiency in conjunction with our Affiliate University.

Stage 3: Advanced: Student teachers, staff and other stakeholders shall use different applications software to enhance their own learning through: database applications,

teaching and learning, assessment practices, analysis of data and problem solving, computing, design, graphical and audio-visual communication.

C. ICT-ENABLED TEACHING AND LEARNING PROCESSES

ICT-enabled teaching and learning encompasses a variety of techniques, tools, content and resources aimed at improving the quality and efficiency of the teaching and learning processes, ranging from the projection of media to support a lesson, multimedia self-learning modules, simulations, virtual learning and variety of options available for the staff to utilise various ICT tools for effective pedagogy:

i. Availability of a wide range of instructional resources will catalyse transformation of learning environments into ICT-enabled ones.

ii. Tutors will have to participate in selection and critical evaluation of digital content and resources and also be encouraged to develop their own digital resources and share with colleagues, student teachers and other stakeholders where necessary through the digital repositories.

iii. Computer laboratory shall serve as a teaching and learning hub for ICT and progressively extend to other learning environments in course of time.

iv. ICT instructors with appropriate qualifications shall manage the ICT laboratory.

D. ICT FOR SKILL DEVELOPMENT

i. The College in collaboration with the affiliate University shall organise certificate courses in ICT education in the community.

ii. Job-oriented courses in ICT shall be designed with the affiliate University to improve ICT integration and literacy skills for staff and students.

iii. These certificate courses will be frequently revised and updated in order to maintain relevance to changing requirements of the job market and emerging trends in technology.

iv. An open-learning system (virtual) will be developed permitting students to ensure continuous learning outside campus.

E. ICT FOR INCLUSIVE EDUCATION

i. The College shall use ICT to facilitate inclusive education.
ii. ICT software and tools such as screen readers and voice readers shall be used to enhance access to persons with disabilities.
iii. Staff shall be sensitized on issues relating to special needs and develop possible ICT tools to address them.

F. ICT FOR LEADERSHIP AND MANAGEMENT

The Leadership and Management of DACE are mandated to adopt the use of ICT as an integral part of the processes and procedures for College service delivery for quality teaching, learning and research. The use of Colleges of Education Management Information System (CEMIS) for:

i. staff records
ii. student records
iii. College data including inventories for resource management
iv. College financial management
v. teaching, learning and research activities

Other associated management practices of ICT

a. Upgrade and update the official College Website to publicise College information and administer electronic mail (e-mail) systems for all College staff and student teachers.
b. Provide basic ICT resources to support academic work especially relating to training student teachers to teach with ICT tools.
c. Provide basic ICT resources to support administrative work.
d. Provide systems for information and resource sharing among staff and student teachers of the College.
e. Establish ICT Centres that support teaching, learning and training.
f. Develop internal acceptable use of the ICT policy.

g. Establish College ICT Steering Committees (CISC) to supervise the implementation of ICT integration in the College.

h. Develop a campus Wireless Local Area Network (WLAN) to enable automation of a variety of processes, beginning with library automation, locally cached offline access to internet resources, office automation, maintenance of records, student tracking, resource planning and assessment, using the existing ICT infrastructure to increase efficiency.

G. ACCESS CONTROL STANDARDS

Access control defines access to computer systems to various categories of users. Access Control Standards are the rules which the College applies in order to control access to its ICT resources. Such standards shall be appropriate to the College's operation and security needs. The dangers of using inadequate access control standards shall range from inconvenience to critical loss or data corruption.

Access Control Standards for ICT resources shall be established by the College ICT Steering Committee **(CISC).** It shall incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet operational needs.

Procedures for Access Control

i. The CISC shall develop access control standards for ICT resource(s) usage in the College.

ii. In addition, increased sensitivity of ICT resources, CISC shall amend Access Control requirement on regular basis.

Managing User Access

The System Administrator shall authorise access to all systems and such access, including the appropriate access rights and privileges shall be recorded in an Access Control List. Such documents shall be regarded as Highly Confidential and safeguarded accordingly.

Good management of user access to ICT resources shall allow the implementation of stringent security controls and to identify breaches of Access Control standards. Access control issues to be considered, when implementing this procedure, include the following:

i. Inadequate management of access control procedure could result to unauthorised access to ICT resources, which could compromise data confidentiality and integrity.

ii. Informal documentation and access control can frustrate re-allocation of duties where there are no regulation and documentation of Access Control rights and privileges.

iii. An unauthorised user can gain access to user identification and authentication about the system prior to successful logon if the logon screens or banners are not removed.

iv. Unapproved allocation of privileges to staff can result in abuse of Access Control Standards.

Procedures for Managing User Access

i. All users shall be defined by unique logon credentials with specific defined privileges.

ii. The College shall have an account removal process for persons who are no longer members of the College.

iii. All users shall avoid logon screens or banners which supply information about the system prior to successful logon, as they can assist unauthorised users to gain access.

iv. There shall be no allocation of inappropriate privileges to staff.

Managing Network Access Controls

Access to the ICT resources on the network shall be strictly controlled to prevent unauthorised access, and access to all ICT resources shall be restricted unless explicitly authorised.

Connections to the College networks shall be properly managed to ensure that only authorised devices or persons are connected. Information Security issues to be considered when implementing this procedure shall include the following:

i. Unauthorised access to programs, applications and systems could result in fraudulent transactions or entries such as modification of data, fraudulent e-mail used, etc.

ii. Where physical or logical access has not been controlled, users may find and exploit

inadvertently access routes to College systems and network resources.

iii. Changes made to a network access profile without appropriate change control procedures could lead to unintended and possibly accidental access to unauthorised network resources.

iv. All connections to a third-party network may not only introduce malware but can also interfere with business processes where data is transmitted unintentionally to the network.

v. User Identification and authentication that indicates user's privileges can allow hackers to crack their password.

Procedure for Managing Network Access Controls

i. All campus network devices and system must be linked to the domain controller and all users monitored on the networks.

ii. Physical or logical and program access must be regulated and controlled by the Systems Administrator.

iii. The System Administrator is responsible for granting access to external users of the campus network.

iv. User Identification and authentication that indicates user's privileges must not be allowed.

v. All connections to a third-party network must be under the control of the system administrator.

vi. Revisions to a network access profile must be made using authorised change control measures.

Operating System (OS) Software Access Control

The operating system controls a computer's operation; 'pre-loaded' with commands and utilities which set-up and maintain the computer's environment.

Access to operating system commands shall be restricted to those persons who are authorised to perform systems administration/management functions. Such access shall be operated under dual

control requiring the specific approval of the College's Senior Management Official(s).

All systems and ICT equipment shall be secured to ensure the safety of all development tools and utilities prior to delivery to end-users.

Information security issues to be considered when implementing this procedure shall include the following:

i. Users accessing the command line should not be able to execute system command that could damage and corrupt the program and data file.

ii. Operating system commands as well as other system vulnerability may be used to disable or by-pass access control and audit log facilities.

Procedures for managing OS access control

i. Access to the command line of the Operating System shall be restricted to general users.
ii. Operating system command and access control must be under the guidance of the system administrator.

H. SECURING AGAINST UNAUTHORISED PHYSICAL ACCESS

Physical access to high security areas shall be controlled with strong identification and authentication techniques. Staff with authorization to enter such areas shall be provided with information on the potential security risks involved.

Personnel who work in, or have access to high security areas may be put under pressure within or outside the College to reveal access codes or keys, or to breach security by performing unauthorised/illegal tasks, such as copying confidential information. The College shall provide adequate information regarding these threats to prevent such eventualities. Security aspects shall be designed in such a manner that the responsibility of high security data can be accessible among various officers.

In case security breach occurs at one level, it can be prevented on other levels. The application shall have multilevel password authentication.

Procedures for Physical Access Control

i. All buildings where ICT resources are kept shall be adequately secured and only authorised personnel shall be allowed into Server Rooms and Networking Operating Centres.
ii. Students and staff shall only be given access to ICT Centres under the supervision of administrators.
iii. Notices shall be placed at restricted areas to inform and prevent unauthorised access.
iv. Authorised personnel who manage ICT Centres shall monitor and ensure that ICT resources are used for the intended purpose(s).

I. E-MAIL

There shall be creation of institutional e-mails for all Departments, Units, Staff and Students. Compliance to this procedure shall help the College to:

i. improve the successful delivery of College communications to and from all departments, units, staff and students.
ii. reduce the risk of College data classified as Legally Restricted or Confidential from going through e-mail systems.

USE OF E-MAIL ACCOUNTS

All staff and students shall use only the institutional e-mails for official communications.

Personal use of institutional e-mail is allowed, provided that the use:

i. does not materially interfere with performance of work responsibilities;
ii. does not interfere with performance of the College networks, and it is otherwise in compliance with this and other College policies.

Procedure for proper use of E-mail

i. Unsolicited electronic mail (i.e., SPAM) shall not be acted upon or forwarded. If data users fear they may have responded to SPAM e-mails, they should contact the System Administrator immediately to have their user authentication updated.
ii. Misuse of institutional E-mail

Misuse of Institutional E-Mail

Any policy of the College that applies to communications also generally applies to e-mail. Use of institutional e-mail in violation of other College policies is also a violation of this procedure.

The following shall constitute misuse of the institutional email:

i. Concealment or misrepresentation of identity or affiliations; for instance, misrepresenting oneself as another user.
ii. Use of institutional e-mail to send SPAM
iii. Alteration of source or destination address of e-mail.
iv. Use of e-mail for harassment and discrimination.

Selection and Management of Passwords

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. Passwords shall not be shared with any other person for any reason. Most computer systems are accessed by a combination of User ID and password. This procedure outlines the management of passwords from a System Administrator's perspective.

Information Security issues to be considered when implementing this procedure shall include the following:

i. Dummy passwords allocation via the System Administrator or ICT instructor can compromise access control.

ii. Passwords that are shared may allow unauthorised access to the information systems.

iii. Users who need to access multiple systems may keep a hand-written note of the different passwords. However, such insecure records make an easy target for ill-intentioned persons wishing to break into the system.

Procedure for Managing Passwords

i. All default passwords shall be changed after first log-on.

ii. This shall be made of alpha-numeric, special characters with minimum of 8 characters.
iii. All passwords shall be changed regularly and not be shared.
iv. Third party password managers shall be disabled on all systems.
v. Users shall be sensitised on password vulnerability threats.

J. ACQUISITION OF ICT RESOURCES

This section offers a guideline for acquiring/purchasing ICT resources to ensure that they are suitable for the College, provide value for money and integrate with other College technologies where applicable.

Procedures for Acquisition

The System Administrator in consultation with the ICT Unit shall ensure that:

i. There is a defined minimum specification for the acquisition of new hardware.
ii. All computing devices purchased are suitable to run all operating systems and Application software relevant to the needs of the College as well as integrate with other existing hardware.
iii. All purchases are in line with the procurement procedures of the College.
iv. There is a defined minimum specification for the acquisition of College Software (Off-the-shelf and Open Source).
v. Quality Assurance Unit of the College shall perform a system audit at the beginning of every semester and recommend appropriate actions for the attention of College Management.
vi. The CISC ensures the interoperability of ICT resources in the College.

Hardware

i. The College Management shall supply ICT infrastructure to equip the ICT Unit to keep the unit in active use. At least, one printer, a scanner, a projector, a digital camera, an audio recorder and such other devices are part of the infrastructure.

ii. Computer access points with internet connectivity shall be provided at the Library and the College Administration to facilitate an effective and efficient Management Information System.

K. SOFTWARE

This section provides guidelines on the use of software by staff, student teachers and other stakeholders of the College to ensure that all software are properly used. The use of all open source and freeware software shall be conducted under the same procedures outlined for commercial software.

Procedure for Software Licensing

i. All software used by the College shall be appropriately licensed.
ii. All computer software copyrights and terms of all software licenses shall be followed by staff, students and other stakeholders of the College.
iii. Where licensing states limited usage for number of computers and/or users, the System Administrator shall ensure these terms are complied with.
iv. The College website shall conform to the NITA Act 771 (2008).
v. All software shall be properly registered, installed on the College system and owned by the College.
vi. All software installations and updates shall be carried out by the System Administrator/ICT instructors.
vii. Prior to the use of any software, staff, student teachers and other stakeholders of the College shall receive orientation on the use of software.
viii. Where applicable, written approval from the College Management shall be obtained before software is installed on personal devices.
ix. Unauthorised duplication, acquisition or usage of software copies are prohibited.

Breach of Software Procedures

i. No user of the College software/network shall breach software user regulations.
ii. Where a member of the College community becomes aware of a breach of the use of software in accordance with this procedure, he or she is obliged to notify the System Administrator immediately.

iii. The System Administrator, at the point of identifying the issue(s) on the breach of procedures by staff, students and other stakeholders, shall refer the incident to the Principal within forty eight (48) hours for action.

6. INCLUSION RESPONSIVE STATEMENT

All provisions made by this policy shall apply to all manner of persons considered stakeholders of the College irrespective of their gender, ethnicity, religion, social status, ability and cultural background and affiliations in such a manner that no act of discrimination is promoted under any circumstance in any engagement of the College.

7. RESPONSIBILITY FOR IMPLEMENTATION

a. The Academic Board
b. The Academic Planning and Quality Assurance Committee
c. The Mathematics/ICT Department

8. RESPONSIBILITY FOR MONITORING

a. The Principal
b. The Academic Board
c. The Academic Planning and Quality Assurance Committee

9. KEY STAKEHOLDERS

a. The College Governing Council
b. The Mentoring Universities
c. The Academic Board
d. The College Management
e. The Staff
f. The Students
g. The Students' Representative Council

10. STATUS

Approved

11. INITIATING BODY

a. The Academic Board
b. The Academic Planning and Quality Assurance Committee
c. The ICT Unit

12. SPONSOR

The College Principal

17. AUTHOR

The College Principal

10. APPROVAL BODY

The College Governing Council

14. EFFECTIVE DATE

16th September, 2020

15. REVIEW DATE

2023

16. RELATED LEGISLATION

Colleges of Education Act, 2012 (Act 847)
National Information Technology Act, 2008 (Act 771)

17. RELATED POLICY

a. Harmonized Statutes for Colleges of Education, Ghana

b. NCTE ICT Integration Policy for Colleges of Education, Ghana

18. FURTHER INFORMATION

For further information or enquiries regarding this policy, please contact the following:

The Principal
Dambai College of Education
P. O. Box 84
Dambai
Oti Region
Ghana
West Africa
dace74dambai@gmail.com/info@dace.edu.gh
0243125225
0242080370