DAMBAI COLLEGE OF EDUCATION

DATA SECURITY POLICY

DACE/DSP001/2020

TABLE OF CONTENTS

DATA SECURITY POLICY

DACE/DSP001/2020

1. INTRODUCTION

Dambai College of Education will obtain, use, store and otherwise Process Personal Data in order to carry out its functions. When processing Personal Data, the College is obliged to fulfill individuals' reasonable expectations of privacy by complying with the General Data Protection Regulation [GDPR], (ref. Data Protection Act 843) and other relevant legislation and regulations.

The purpose of this policy is to outline essential roles and responsibilities within the College Community for creating and maintaining an environment that safeguards data from threats that will endanger personal, professional and institutional interests and to establish a comprehensive data security program in compliance with applicable laws.

2. THE POLICY STATEMENT

Data Security and Protection is the major challenge of ICT in contemporary times. For the College to use ICT for its intended purposes, a robust ICT system will be developed in the College such that an individual in each department/unit privy to College Data will be assigned user identification and authentication which must not be divulged to anyone, including ICT support services staff, for any reason. User identification and authentication for the College systems should not be used for any other service. To ensure a security of data, there is a need for a clear guideline on the handling of College data by providing the needed environment for this purpose. This policy therefore prescribes mechanism for data security in the College.

3. OBJECTIVES

The policy objectives are to:

a. Create safe data environment from personal, professional and institutional threats.
b. Establish a comprehensive data security program for the College.
c. Provide support and services to enable staff and student teachers handling personal and College's data to remain compliant with the legislation and the College's requirements in respect of data security.

4. SCOPE

i. This policy applies to staff, whether full- or part-time, paid or unpaid, temporary or permanent, student teachers, former staff, website users, research subjects, contractors, and other stakeholders of the College.

ii. This policy applies to all information collected, stored or used by or on behalf of any operational units, departments and persons within the College in connection with its operations.

5. SUPPORTING PROCEDURE

A. Data Classification

All pieces of information covered by this policy are classified among four categories, according to the level and the security necessity in the College. In descending order of sensitivity, the categories are “Strictly Confidential,” “Confidential,” “Internal Use Only,” and “Public Use.”

a. Strictly Confidential Information includes any information that the College has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. Strictly Confidential information must be given the highest level of protection against unauthorised access, modification, or destruction. Unauthorised access to Strictly Confidential information may result in a significant invasion of privacy or may expose members of the College community to significant financial or academic risk. Without limiting the generality of the foregoing, Strictly Confidential information shall include “personal information”, customer information, medical or health information pertaining to members of the College community and data collected in the course of research on human subjects. In addition, Strictly Confidential information also includes export-controlled information, and other sensitive information that the information sponsor or the Principal has determined must remain on a secure College server.

b. Confidential information includes sensitive personal and institutional information. Unauthorised access or modification to personal Confidential information may adversely affect individuals. Unauthorised access or modification to institutional Confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of the College.

Examples of Personal Confidential Information include:

i. information protected under privacy laws
ii. information concerning the pay and benefits of College employees
iii. employee performance appraisals for current, former and prospective employees
iv. donor addresses and gift data
v. College financial and planning information
vi. legally privileged information
vii. invention or discovery disclosures
viii. other information concerning pending patent applications
ix. personal certification
x. regulatory reporting
xi. online course evaluations
xii. students records

c. Internal Use Only information includes information that is less sensitive than Confidential or Strictly Confidential information, but that, if exposed to unauthorised parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of the College.

d. Public information is information that is generally available to the public, or that, if it were, to become available to the public, would have no material adverse effect on individual members of the College community or upon the finances, operations, or reputation of the College.

e. In the event where information is not explicitly classified, it is to be treated as follows:

i. Any data which includes any personal information concerning a member of the College community (including any health information, financial information, social security numbers or other personal identification information) shall be treated as Strictly Confidential information.

ii. Any data which includes academic evaluations or other academic records shall be treated as Confidential information.

iii. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

f. The Data Security Committee may from time to time provide clarifications relating to the security classifications, and may, through issuance of Data Security Directives establish more detailed requirements concerning the classification of Information Resources, Information Systems, or Specific Data.

B. Specific Data Security Procedures

i. Designating and managing the efforts of one or more Sponsors and Data Security Officers for all Information Resources maintained in their area of responsibility.

ii. Approving access authorisation of all Users of Information Resources maintained in their area of responsibility having data classification of Strictly Confidential Data Security Procedures.

iii. Ensuring that Strictly Confidential, and Internal Use of data sponsored within their area of responsibility are not provided or accessible to, or created or maintained by College vendors or other third-parties.

iv. Monitoring for risks to data security and reporting any known or reasonably foreseeable risks to the College.

v. Ensuring that users comply with all security-related procedures pertaining to any Information Resource to which they have authorised access or any information derived from there.

C. Data User Responsibility:

Individuals using any College data shall be responsible for:

i. becoming familiar with and complying with all relevant College policies, including, without limitation to this policy, and all other policies related to data protection and integrity, technology use and privacy rights.

ii. providing appropriate physical security for information technology equipment, storage media, and physical data.

iii. Ensuring that Strictly Confidential, or Internal Use Only information is not distributed or accessible to unauthorised persons.

iv. complying with this Policy and all relevant Data Security Directives irrespective of where the College information or data might be located on personal devices, the Internet, or other third-party service providers.

v. disposing of College data/information that may not be needed in a manner that insures against unauthorised interception of any Strictly Confidential, or Internal Use Only information.

D. Security Breach Response

i. Users must report any known Security Breach or any incident that is likely to cause a Security Breach. These may include thefts of computer devises, viruses, tempering with results, hacking the system, pornographic, worms, or computer “attacks” that may lead to unauthorised access to non-Public information.

ii. Immediately upon becoming aware of a likely Security Breach, the ICT Unit shall conduct an investigation commensurate with the nature of the breach and report to the College Management for actions.

iii. The ICT Unit shall conduct a post-incident review of events and determine what, should any changes be made to College practices or policies to help prevent similar incidents.

E. Enforcement Sanctions

The College reserves the right to monitor network traffic, perform random audits, and to take other steps to ensure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result in dismissal from the College.

6. INCLUSION RESPONSIVE STATEMENT

All provisions made by this policy shall apply to all manner of persons considered as 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
Dambai
Oti Region
Ghana
West Africa

dace74dambai@gmail.com/info@dace.edu.gh

0243125225

0242080370