TAKORADI TECHNICAL UNIVERSITY

DATA MANAGEMENT POLICY

Takoradi Technical University
P. O. Box 256,
Takoradi - Ghana,
West Africa.

Website: www.ttu.edu.gh
Email: info@ttu.edu.gh/ info@tpoly.edu.gh
Tel: +233 (0) 312 025 162
Fax: +233 (0) 312 025 256

TABLE OF CONTENTS

1.0 Introduction

Takoradi Technical University operates in an increasingly complex, data-oriented environment that requires the effective collection, management, analysis and dissemination of data. The data generated and held by the University are key assets that must be managed correctly to underpin the University's strategic development, essential functions and academic integrity.

All data created and acquired shall be owned by the Takoradi Technical University and shall remain as the property of the University and shall be classified as corporate assets.

2.0 Guiding Principles

1. In order for the University to effectively manage and safeguard its data assets, procedures shall be put in place to guide appropriate data access, ensure the security of the data, and provide a means to address procedural exceptions.

2. Roles, including those of individuals with data responsibilities and of eligible users, are necessary to support data integrity and security.

3. Sharing information across organizational boundaries shall be facilitated where appropriate.

4. A sustained data administration function shall reinforce a set of definitions for commonly consumed data, with the understanding that there may be multiple valid definitions.

5. Data integration across the University shall be encouraged to foster data accuracy and uniformity, and demonstrate an understanding of the Institutional complexity, various data systems, and differing data formats.

3.0 Objective

The University values access to timelines, accuracy, and consistency of information, while fully appreciating the basic security and privacy requirements involved as stipulated in the Takoradi Technical University Data Protection Policy. Controlled access by staff to administrative information is necessary in order to support University functions. Shared definitions for data and appropriate roles have been developed to support the use of University data and the University Data Warehouse.

4.0 Scope

The University's Data Management Policy applies to all staff whose job responsibilities include inputting data into or retrieving data from University's data systems, or using data from the University Data Warehouse, and those who supervise such individuals. It also includes;

i. Data, in all its forms, required for the management and ad ministration of the University and the conduct of its work, whether the data are captured and accessed from on-campus or off-campus locations.

ii. All University activities.

iii. Collaborative activities undertaken with partner organizations.

iv. The management of research data.

5.0 Definitions

5.1 Data: Distinct units of information such as facts, numbers, letters, symbols, usually formatted in a specific way, stored in a database and suitable for processing by a computer and/or assigned personnel.

5.2 Data Quality: This refers to the accuracy, completeness, validity and currency of the data.

5.3 Data Integrity: This refers to the attribute of data that has not been altered or destroyed in an unauthorized manner.

5.4 Dataset: A defined collection of data with common elements related to a specific function;

5.5 Data Dictionary: A file that defines the basic organization of a database containing a list of all files in the database, the number of records in each file and the names and types of each field.

5.6 University Data: Data gathered, produced, stored, and/ or disseminated concerning any aspect of the University's operations, also referred to as Institutional Data.

5.7 University Data Warehouse: The repository for University data, which is used for reporting both transactional and analytical data.

5.8 Data User: Authorized individuals or staff who access University data in order to perform their assigned duties and for purposes provided for by this policy.

5.9 Information: data combined and processed into a meaningful form.

5.10 Information System: a computer system used to gather, store, structure, secure, process, combine and filter data into information and that makes that information available on time and in a useful form for users and institutional requirements.

5.11 Data Management Framework: The organizational structure in place to manage the University's data assets.

5.12 Data Advisory Committee: A senior level team comprised of the Data Trustees and Data Stewards that is responsible for the overall management of University data. The committee is charged with the operational effectiveness of data management policies.

5.13 Data Trustees: Senior University officials who have planning and policy-making responsibility for the University Data Warehouse.

5.14 Data Steward: The person responsible for the operational management and processing of the data in an information system who has detailed knowledge and experience in the operational management and use of specific Datasets and their structures, capture, administration, processing and reporting.

5.15 Hard Copy Data are data produced on paper or other tangible devices.

5.16 Soft Copy Data are data that are intangible except produced on output devices and can be kept on storage devices.

6.0 DATA ADMINISTRATION

6.1 General University Access

All Data Users without restriction shall access data categorized as General University Access.

6.2 Limited Access

At the absolute discretion of the University, specific data shall be categorized as 'Limited Access'. Data will be categorized as 'Limited Access' by the Planning Officer in the light of recommendation from Data Stewards and where appropriate, legal and other advice.

Considerations that should go into categorizing data as 'Limited Access' includes but not limited to personal privacy, legal require-

ments, commercial confidentiality, security, externally imposed constraints or other recognized good reason.

6.3 Public Access

Data, which at the absolute discretion of the University, are determined to be a matter of public record and can therefore be made freely available without restriction are categorized as Public Access.

Data will be categorized as 'Public Access' by the Planning Officer in the light of recommendations from Data Stewards, Freedom of information requirements, Data Protection Act and where appropriate, legal and other advice.

6.4 Protected Data

Data that require a higher level of classification than public data such as Confidential and Restricted Data;

6.4.1 Confidential Data

Data categorized as 'Confidential Data' may be data that would not be made available or disclosed to unauthorized individuals, entities or processes for legal and or business reasons.

6.4.2 Restricted Data

Data to which access is subject to special controls for reasons of security or safeguarding the data.

6.5 Ownership of University Data

All University Data are owned by Takoradi Technical University. As such, all members of the University community have the obligation to appropriately respect and protect the asset, in all formats and in all locations.

6.6 Data Steward

Data Stewards are responsible for and accountable to the relevant

Data Trustees for:

6.6.1 Developing a data access plan in consultation with the ICT Board.

6.6.2 Creating and performing processes to capture and fix inconsistent or erroneous data.

6.6.3 Certifying published reports and analytics.

6.6.4 Certifying data reposted in the University Data Warehouse.

6.6.5 Participate in security access audits.

7.0 DATA CLASSIFICATION

The University Data shall be categorized as Limited, Restricted, Protected, Confidential or Public and shall be safeguarded appropriately.

7.1 Access and Confidentiality

Access to University data shall be based on the business needs of the University and should enhance the ability of the University to achieve its mission. The University staff shall have access to the data needed to perform their responsibilities without regard to arbitrary barriers and in many cases that data need not be individually identifiable. The University Data Warehouse shall be built taking into account these factors.

Because no computer system is completely immune from exploitation, applying layered security controls will better safeguard University computers and the University's ever-expanding body of sensitive data/information. In order that the proper controls are applied, it is the responsibility of each individual utilizing University computer and data resources to:

i. Know the classification of the system being used.
ii. Know the type of data being used.
iii. Follow the appropriate security measures.
iv. Consult the 'Related Policies' at the end of this policy for further information.

Beyond existing policies, specific policies implementing data access and security, including within the University Data Warehouse, developed by functional areas, need to be approved by the Data Advisory Committee to ensure consistency with the Guiding Principles, set forth in Section A, above.

7.2 Training

Before individuals will be allowed to access University data, training in the use and attributes of the data, functional area data policies, and University policies regarding data is mandatory.

7.3 Master (Metadata) Standards and Definitions

A terminology/taxonomy shall be developed by the Data Advisory Committee, or an appropriate subset, in order to provide a framework for requesting and producing consistent data across all levels of the University. The definitions shall be accessible to all University data users and shall be included in training programmes.

7.4 Integrity, Validation, and Correction

Data, as a University asset, shall be safeguarded and managed at all points and across all systems, from creation to use, to archive, through coordinated efforts and shared responsibilities, to ensure their accuracy. Each functional area will develop and implement processes for identifying and correcting erroneous or inconsistent data. When and if erroneous or inconsistent data have been identified, the Data Steward from the corresponding functional area shall within five working days either correct the data or refer the issue to the appropriate office. The University Planning Office

shall develop and implement data auditing processes.

7.5 Extraction, Manipulation, and Reporting

Extraction, manipulation, and reporting of University data shall be done only for University business purposes and for any other purpose authorized by the University through a responsible officer.

i. Unauthorized personal use of University Data, including derived data, in any format and at any location, is prohibited.

ii. Where appropriate, before any information is used outside the data user's functional unit, verification with the functional area manager is recommended.

7.6 Retention and Archiving

Data considered for retention and archiving shall be categorized into two; Hard Copy data and Soft copy Data. Hard Copy data shall be retained and archived for a minimum of fifty (50) years and all unsuccessful application data for a minimum of six (6) months or otherwise as may be recommended by the Data Advisory Committee in consultation with the University Management. The University shall provide a well-designed structure or facility to accommodate the storage of hard copies of archived staff and institutional documents for not less than fifty (50) years. Such structure or facility shall be well secured for both fire and water prevention. Soft Copy data can be retained and archived as long as may be recommended by the Data Advisory Group. The archiving software shall be updated at most every two years and or as shall be recommended by the Data Stewards.

7.6.1 Exemptions:

Examinations scripts and any other documents with affiliation to external bodies would be subject to the data rules of those bodies.

7.7 Access to University Data from Global Locations

As the University continues its evolution as a Global Centre of Higher Learning, all remote sites shall need to access University data following the same policies as well as the policies of these sites / subsidiaries and where the data policies of these sites / subsidiaries conflict with the University's policies, policies of the University shall take precedence.

7.7.1 Exceptions to Standard Data Access

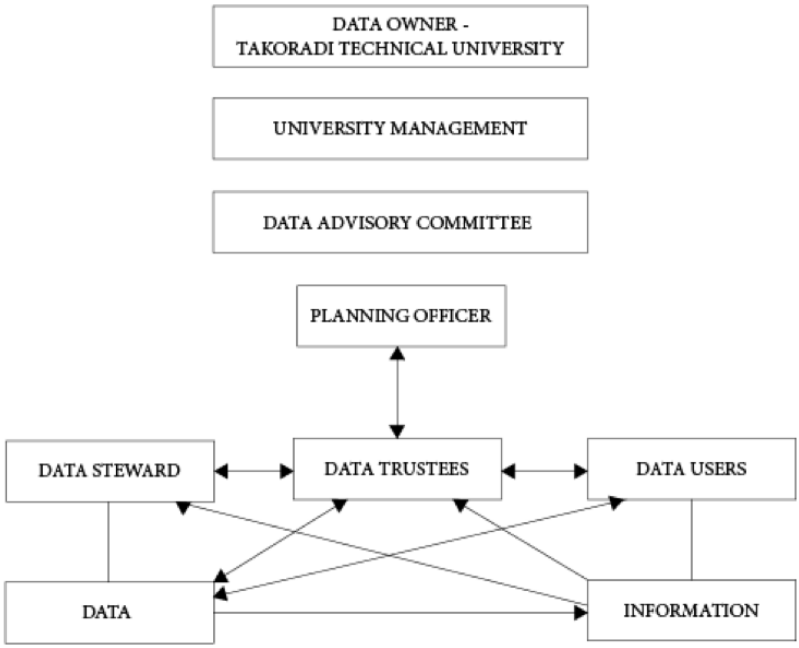
Procedures shall be developed to address those cases where an individual seeks permission to access data outside of the access plan and defined roles. In those instances, the individual shall submit a written request seeking non-standard access. This request shall include a statement indicating the access being sought and the reason for the request, and shall be submitted to the Chairperson of the Data Advisory Committee. The Chairperson shall send the request to the appropriate Data Steward for review and decision. The Data Steward shall report the decision to the appropriate Data Trustee and to the superior officer where applicable.

8.0 DATA MANAGEMENT ROLES AND RESPONSIBILITIES

To support an effective University data administration and management programme, a series of data management roles are outlined below:

8.1 Data Management Framework

The following structure forms an institutional Data Management Framework, the purpose of which is to ensure data are consistent, of good quality and available for use by Data Users.



8.2 Data Owner

Takoradi Technical University.
University Management
University Management is Top Level Management officers who have executive policy-making responsibility for the University.

8.3 Planning Officer

Planning Officer shall be a senior University official who is responsible to the Vice Cancellor and the Data Advisory Committee for data owned and managed by the University, for data management policy, standards and procedures. The Planning Officer shall develop a University data model, promote, implement, monitor and review the effectiveness of data management policy, standards and procedures in the formulation of data management policy and standards for the approval of University management.

8.4 Data Trustees

Data Trustees shall be senior University officials who have planning and policy-making responsibilities for University data and the Data Warehouse. The Data Trustees shall be responsible for overseeing the establishment of data management policies and procedures, and for the assignment of data management accountability. Data Trustees shall be composed of Heads of Department of Planning, ICT, Quality Assurance Office, Industrial Liaison Office, Deputy Registrars, the Librarian and Vice Deans.

8.5 Data Stewards

Data Stewards are typically operational heads in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the transaction processing systems. Data Stewards shall be appointed by the respective Data Trustees. Data Stewards' responsibilities shall include the data management activities outlined in this policy and other activities shall be assigned by a Data Trustee. Data Stewards shall be responsible for defining the criteria for archiving data to satisfy retention requirements. Data Stewards shall have the responsibility to establish the processes for documenting data elements.

Data Stewards will be responsible for developing an overall data access plan. The plan should outline various roles and the access each role will have to data, including within the University Data Warehouse. Data Stewards shall seek to balance the need for information to perform one's job responsibilities and to ease administrative functionality with the need for keeping data confidential and secure. Data is categorized as Restricted, Protected, Confidential or Public. The data access plan shall consider the categorization of the data in developing each access role.

Data Stewards' responsibilities include, but are not limited to:

i. The operational management of the data assigned to them and their integrity.

ii. Apply University data management standards and procedures.

iii. Effectively liaise with the technical experts responsible for the repositories where the data are stored and for the applications and reporting systems for use of the data.

iv. Data analysis.

v. Provide management information to support University decision-making.

vi. Create and perform processes to capture and fix inconsistent or erroneous data.

vii. Implement an agreed data retention criteria and archiving policies.

viii. Make the Data Dictionary understandable to users.

ix. Develop a data access plan.

x. Certify published reports and analytics.

xi. Certify data reposted in the University Data Warehouse.

xii. Participate in security access audits.

In support of the role of the Data Steward, the ICT officer of the University shall provide ICT services.

8.6 Data Users

Data Users are authorized individuals or staff who access the University data to perform their assigned duties and for purposes provided for by this policy. Data Users shall be responsible for

protecting their access privileges and for the proper use of the data they access.

8.7 The University Planning Office

The Planning Office shall work with the appropriate Data Stewards to develop definitions of commonly used terms such as "department" and "enrolled student." In addition, the Planning Officer, with the appropriate Data Stewards, and using his/her knowledge of external reporting requirements and standards, shall define how official University metrics are calculated (e.g., if calculating space per student, what type of space is included in the calculation [all space, academic space, etc.] and which student count is used. Further, in the course of his/her work, the Planning Officer shall typically discover data discrepancies and inconsistencies and shall promptly report such to the appropriate Data Steward for resolution.

8.8 Data Advisory Committee

The Data Advisory Committee shall establish overall policies for management and access to the University Data. This committee shall be composed of two representatives from Planning Office, Registry, Quality Assurance Office; and one each from ICT and Library, and all the Vice Deans.

This committee shall see to the development of data management standards and procedures in each functional area to ensure appropriate compliance and review their operational effectiveness for purposes of improvement or change. It shall ensure effective oversight of all University processes that capture, maintain and report on data used in the University's data driven decisions. In addition, the committee shall ratify definitions of commonly used terms and metrics. The committee shall be chaired by the Planning Officer.

9.0 UNIVERSITY DATA WAREHOUSE

9.1 Data Warehouse

The University Data Warehouse shall exist to support Data User queries to track and respond to business trends, to facilitate forecasting and planning efforts, to produce reports, and to store sharable data from operational systems-of-record. The University Data Warehouse shall serve as the University repository from which official information is produced. The accuracy of data that is reposted in the University's Data Warehouse shall be certified by the responsible Data Steward.

9.2 Training

Before individuals shall be allowed to access the University Data Warehouse, training in the use and attributes of the data, the data retrieval tools, functional area data policies, and University policies regarding data shall be mandatory.

9.3 Extraction, Manipulation, and Reporting

Extraction, manipulation, and reporting of data from the University Data Warehouse shall be done only for purposes approved by the University.

a. Personal use of University Data, including derived data, in any format and at any location without express permission from the University is prohibited.

b. Where appropriate, before any information from the University Data Warehouse is used outside the Data User's functional unit, verification with the functional area head is recommended.

9.4 Storage

There shall be only one official data repository for storing data which is the University Data Warehouse. To the extent possible, data element names, formats, and codes shall be consistent across all applications which use the data, as well as with University stan-

dards.

9.5 Data Documentation

Data Stewards shall be responsible for establishing the processes for documenting data elements in the University Data Warehouse. Documentation of derived data shall include the algorithms or decision rules for the derivation. The University ICT shall specify a standard data format for receiving and entering data definitions and descriptions into a metadata repository.

9.6 Related Policies

1. Takoradi Technical University Admission Policy
2. Takoradi Technical University ICT Policy
3. Takoradi Technical University Examination Policy
4. Takoradi Technical University Research Policy
5. Takoradi Technical University Industrial Liaison Policy

10.0 DATA PROTECTION

10.1 Introduction

The Data Protection Act 2012 regulates the way in which certain information is held and used. Although the Act does not currently apply to most of the records about staff and students held by the University, we consider that many of the principles in the new Act represent best practice and we have therefore decided to issue this policy to all staff and students.

This policy gives some useful information about the type of information that the University keeps about you and the purposes for which the institution keeps that information. This policy gives direction to the Data Management Policy and other policies related to data management in the University.

Throughout one's employment or training and for as long a period as is necessary following the termination of one's employment or training, the University would keep information about one for purposes connected with one's employment or training, including

one's recruitment and termination of one's employment or training.

10.2 Types of Information Held (Staff and Students)

10.2.1 Staff

The records may include:

1. Information gathered from one and any references obtained during one's recruitment.
2. Details of one's terms of employment.
3. Payroll details.
4. Tax and insurance information.
5. Details of one's job duties.
6. Health records.
7. Absence records including holiday records and self-certifica tion forms.
8. Details of any disciplinary investigations and proceedings.
9. Training records.
10. Contact names and addresses.
11. Correspondence with the University and other information that one has given to the University.

10.2.2 Students

1. Admission Form
2. Academic Records after graduation (Minimum 5 years, Maximum 10 years) to be referred.
3. Students Trust Loan information.
4. Medical Reports.
5. Disciplinary Records.
6. Awards (Academic and Others)
7. Students Leadership
8. Membership of Committees

10.3 Use of Information

The University shall recognise that these uses are consistent with employment or training relationship and with the principles of the

Data Protection Act 2012. The information held by the University shall be used for management, administrative and research purposes only. The University shall from time to time, disclose some information held about staff/students to relevant third parties (for example where legally obliged to do so by the Ghana Revenue Authority, National Security or where requested to do so by you for the purpose of giving a reference). The University shall also transfer information about staff/students to entities having business dealings with the University solely for purposes connected with one's career or the management of a section of the University.

10.4 Personal Information

Staff/students shall also be aware that the University shall hold information for which disclosure to any party will only be made when strictly necessary for the purposes set out below:

1. For the purposes of compliance with the University's health and safety obligations;

2. For the purposes of management and administration, for example, to consider how one's health affects one's ability to do one's job, or participate in a training programme, and, if one is disabled, whether one requires any reasonable adjustments to be made to assist the person at work or during his or her training programme; and the administration of insurance, sick pay and any other related benefits in force from time to time.

3. In connection with unspent convictions to enable us to assess your suitability for employment.

10.5 Access Requests

Staff/Students have the following rights upon formal request:

1. To be informed whether personal data is being processed by the University or someone else on its behalf; in addition to being

furnished with the following:

i. Fair Processing of the data.

ii. A description of the personal data being processed.

iii. A description of the purposes for which the data are being processed.

iv. Details of all recipients or classes of recipients to whom they are or may be disclosed.

2. To receive communication, in an intelligible form, any information about staff/students held by the University, as well as any information available to the University as to the source of this information. If the information is not in an intelligible form, for instance if it contains codes, staff/students shall be given an explanation of the information. The information shall be provided in a permanent form unless this is impossible, or it would involve a disproportionate effort or you agree to some other form. The copy shall usually be a printed paper copy, but can also be provided in other ways, for example, on disk or via e-mail.

3. To be informed of the logic involved in the taking of a decision that is based solely on the processing by automatic means of personal data, for instance, CV scanning or psychometric testing.

10.6 Repeated Requests

If the University has already complied with an identical or similar request, it shall not be compelled to repeated demands until a reasonable period has elapsed or new information has been added to the file, for example, if the applicant shall be subjected to an investigation or disciplinary hearing, or the information is additional to the one requested earlier.