THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE

PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

TANZANIA PUBLIC SERVICE COLLEGE

(TPSC)

Personal Data Protection Policy

For more Information
Rector/Chief Executive Officer,
Tanzania Public Service College,
P.O Box 2574,
DAR ES SALAAM.

February, 2026

FOREWORD BY THE CHAIRPERSON OF MINISTERIAL ADVISORY BOARD

Tanzania Public Service College (TPSC) is mandated with the personal data of students, trainees, employees, researchers, partners, service providers, visitors, and other stakeholders. The management is conscious about protecting personal data since not only is it a requirement under the Personal Data Protection Act and the Personal Data Collection and Processing Regulations of 2023, but it is a cornerstone of institutional integrity, accountability, and public trust.

This Personal Data Protection Policy reflects the College's commitment to ensuring the lawfulness, fairness, transparency, and security of the processing of personal data, and the maintenance of adequate technical, organizational, and administrative measures to safeguard against any unauthorized access to, disclosure of, alteration of, loss of, or misuse of personal data. This Policy further enhances the College's management of information in respect of the definition of the role of management, staff, trainers, and ICT personnel in the protection of personal data.

I hereby direct all members within the College community and all third-party persons processing personal data on behalf of TPSC to fully comply with this Policy. Together, taking responsibility through collective adherence, the College will safeguard the rights of subjects, improve service provision, and maintain confidence in its core mandate of teaching, research, innovation, and community engagement.

Dr. Florens M. Turuka
Chairperson of Ministerial Advisory Board
February, 2026

PREFACE BY THE TPSC RECTOR &CHIEF EXECUTIVE OFFICER

The Personal Data Protection Policy has been developed to give a clear institutionally defined structure for the collection, processing, storage, sharing, retention, and disposal of personal data collected by Tanzania Public Service College. The policy is informed by data protection policies in place under local legislation.

The policy provides the guiding principles of protecting personal data, the lawful bases of processing, as well as the data controls necessary for achieving data accuracy, confidentiality, data integrity, and data availability. The policy also contains the data subjects' rights, the treatment of sensitive personal data, including biometric and genetic data, the procedure of consent management, data complaints, data breach notification, data protection notices, data protection analysis, third-party data processing, and cross-border data transfer provisions.

The Policy extends to all staff members and students of the College as well as college affiliates and any third-party organization and agents who may process personal data on behalf of the College. There is particular focus on secure environments and extra caution when off-site processing is involved because this exposes data to a higher risk of loss and unauthorized disclosure. There are implementation and monitoring procedures to facilitate compliance and improvement, and this Policy is to be reviewed after three years but earlier when necessary based on the operating context.

The TPSC expresses its appreciation to all stakeholders who have been involved in the formation of this Policy and looks forward to their cooperation during its implementation to ensure that personal data remains handled with integrity, respect, and due diligence.

_____

Dr. Ernest Francis Mabonesho
Rector/Chief Executive Officer
February, 2026

Table of Content

Acronyms

CCTV	Closed-Circuit Television
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
ESS	Employee Self Service portal.
GSO	Government Security Office
HCMIS	Human Capital Management Information Systems
HESLB	Higher Education Students' Loans Board
HR	Human Resource
ICT	Information & Communication Technology
ID	Identification
LGA’s	Local Government Authorities (LGAs)
LMS	Learning Management Systems
MDA’s	Ministries, Departments, and Agencies
NACTVET	National Council for Technical and Vocational Education and Training
NECTA	National Examinations Council of Tanzania
NeST	National e-Procurement System of Tanzania
NIDA	National identification Authority
PDPC	Personal Data Protection Commission
PIA	Privacy Impact Assessments
PO PSM&GG	The President's Office, Public Service Management and Good Governance
R&CEO	Rector and Chief Executive Officer
RRDS	Records Retention and Disposal Schedule
SACCOs	Savings and Credit Cooperative Societies
SIMS	Student Information Management Systems
TAMISEMI	Tawala za Mikoa na Serikali za Mitaa
TCU	Tanzania Commission for Universities
TPSC	Tanzania Public Service College.
VPN	Virtual Private Network
VR	Virtual Reality

Definitions

Anonymization - The process of removing identifying information so that data can no longer be linked to an individual.

College - means Tanzania Public Service College (TPSC)

Consent - A clear, informed, and voluntary agreement by a Data Subject allowing their personal data to be processed.

Data Breach - Any unauthorized access, disclosure, loss, alteration, or destruction of personal data.

Data Controller - The organization or entity that determines the purposes and means of processing personal data.

Data Minimization - The principle that only personal data necessary for a specific purpose should be collected and processed.

Data Processor - A party that processes personal data on behalf of the Data Controller.

Data Protection Officer (DPO) - is an independent, designated officer appointed by an institution to oversee, monitor, and ensure compliance with the Personal Data Protection Act, No.11 of 2022. The DPO serves as the primary focal point for personal data protection matters within the institution and acts as a liaison between the institution, data subjects, and the Personal Data Protection Commission.

Data Subject - The individual to whom the personal data relates.

Personal Data - Any information that identifies or can reasonably identify an individual, directly or indirectly (e.g., name, ID number, contact details).

Processing - Any operation performed on personal data, including collection, recording, storage, use, disclosure, or deletion.

Purpose Limitation - Personal data must be collected for specific, explicit and legitimate purposes and not used beyond those purposes.

Retention Period - The length of time personal data is stored before it is securely deleted or anonymized.

Security Measures - Technical and organizational safeguards used to protect personal data from unauthorized access or misuse.

Sensitive Personal Data - A special category of personal data that requires higher protection, such as health information, biometric data, religious beliefs, or financial details.

Third Party - Any individual or organization other than the Data Subject, Data Controller, or Data Processor that may access personal data.

1. OVERVIEW OF THE POLICY

1.1. Background and Context

The TPSC is committed to protecting individuals' right to privacy in regard to the Personal Data Protection Act, Personal Data Collection and Processing Regulations, 2023. This Policy outlines the College's commitment to lawful, fair, secure, and ethical processing of Personal Data.

The College recognizes that proper and lawful handling of Personal Data enhances institutional reputation, integrity, and trust among students, staff, partners, and stakeholders. During its operations, TPSC processes Personal Data relating to staff, students, trainees, researchers, partners, visitors, and other stakeholders. Such data must be collected and used fairly, stored securely, and not disclosed unlawfully.

The Institution is committed to protecting the privacy, confidentiality, and integrity of personal data belonging to trainees, students, staff, partners, consultants, suppliers, and all those stakeholders whose information is handled by the Institution.

1.2. Purpose of the Policy

The purpose of this Policy is to:

i. Provide principles and procedures for the lawful and secure handling of personal data;
ii. Protect the rights, privacy, and confidentiality of individuals whose data is processed by the Institution;
iii. Outline responsibilities of management, staff, trainers, and ICT personnel in data handling;
iv. Promote accountability and transparency in the Institution's information-management practices;
v. Reduce risks associated with unauthorized access, disclosure, alteration, or loss of personal data.

1.3. Scope

This Policy applies to all processing of Personal Data undertaken by staff, students, and affiliated persons of the College, each of whom is individually responsible for complying with its provisions. As a matter of good practice, any external organizations, contractors, or agents that access or process

Personal Data on behalf of the College are also required to comply with this Policy. The relevant College departments or services engaging such third parties shall ensure that formal written agreements are in place to guarantee adherence to this Policy, supported by applicable procedures, guidance, and advice issued by the Data Protection Officer.

This Policy further applies to all staff and students who process Personal Data off-site. Off-site processing presents heightened risks, including loss, theft, or unauthorized disclosure of Personal Data. Accordingly, staff and students must exercise enhanced care when processing Personal Data at home or in any location outside College premises and shall strictly comply with all applicable ICT management policies, standards, and guidelines, including the Acceptable ICT Use Policy and the ICT Security Policy.

2. POLICY STATEMENTS

The College is committed to protecting the privacy, confidentiality, integrity, and security of all Personal Data entrusted to it by students, employees, researchers, partners, alumni and other stakeholders. In fulfilling its mandate of teaching, research, innovation and community engagement, the College collects, processes, stores, and shares Personal Data in a manner that upholds the highest standards of ethical conduct and complies with applicable national data protection laws, regulatory requirements and international best practices.

2.1. Principles of Personal Data Protection

This Policy establishes the principles, responsibilities, and controls that guide the College in ensuring that Personal Data is:

i. Collected lawfully, fairly and transparently for legitimate academic, administrative and operational purposes;
ii. Processed only for specified, explicit and legitimate purposes, and not used in ways incompatible with those purposes;
iii. Accurate, complete and updated, with measures in place to correct inaccuracies without undue delay;
iv. Protected through appropriate technical and organizational safeguards to prevent unauthorized access, loss, misuse, alteration or disclosure;
v. Stored only for the period necessary to fulfil its intended purpose and in accordance with approved retention schedules;
vi. Accessible to data subjects, who retain the right to inquire, access, update, or request correction of their Personal Data in line with legal provisions;
vii. Shared or disclosed responsibly, ensuring that third parties with whom data is shared uphold equivalent levels of protection;
viii. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
ix. Processed in accordance with the rights of a data subject;
x. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures;
xi. Not transferred abroad contrary to the provisions of the Personal Data Protection Act, Government Notice No. 395B of 2023.

2.2. Data Collection and Use

To collect and process personal data for any specific purpose, the college must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by the college .

2.2.1. Legal Basis for Data Processing

Processing personal data will only be lawful where at least one of the following lawful bases applies:

i. The data subject has given their consent for one or more specific purposes; (*e.g., research participation, marketing communications, use of photos*)
ii. The processing is necessary for the performance of a contract to which the data subject is a party (for instance a contract of employment or registration with the college) ;
iii. To comply with the college's legal or regulatory obligations; such as: national laws on education, employment, taxation, examination standards, reporting obligations to bodies like TCU/ NACTVET/ NECTA, requirements under the national Data Protection and Privacy regulations.
iv. To protect the vital interests of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life e.g., medical emergencies);
v. To perform tasks carried out in the public interest or the exercise of official authority (*generally teaching, research and consultancies)*.
vi. To pursue the college 's legitimate interests where those interests are not outweighed by the interests and rights of data subjects (only available to the college in some circumstances) e.g., CCTV and access control, managing ICT systems, preventing cyber-security threats.

The college must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.
For a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes)
- informed (explained in plain and accessible language)
- unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)
- separate and unbundled from any other terms and conditions provided to the data subject
- freely and genuinely given (there must not be any imbalance in the relationship between the College, and the data subject and consent must not be a condition for the provision of any product or service)

A data subject must be able to withdraw their consent as easily as they gave it. Once consent has been given, it will need to be updated where the college wishes to process the personal data for a new purpose that is not compatible with the original purpose for which it was collected.

2.2.2. Types of Personal Data Collected

The College typically collects the following categories of personal data:
a) Student Data;

- Full name, date of birth, gender, nationality;
- Contact information (phone number, email, address);
- Identification details (NIDA, passport, student ID);
- Academic records (applications, transcripts, exams, results)
- Attendance records;
- Disciplinary records;
- Health information where necessary (e.g., for special needs/medical support);
- Financial information (fees, sponsorship details, bank/payment records);
- Photographs, CCTV footage, biometric data (if used for access control).

b) Staff and Faculty Data

- Personal identifiers (names, date of birth, ID numbers, NIDA);
- Contact details;
- Employment history and qualifications;
- Payroll and financial information;
- Performance evaluation records;

- Medical information required for employment or benefits;
- Disciplinary and compliance records;
- Biometric data used for access or time attendance.
- Photographs, CCTV footage.

c) Visitor and Third-Party Data
- Identification and contact details;
- CCTV recordings;
- Access logs for facilities, events, or online portals.

d) ICT and Digital Learning Data
- Usernames, passwords, login logs;
- Learning management system activity data;
- Email and communication records;
- IP addresses and device information;
- Online assessment submissions and attendance logs.

2.2.3. Methods of Data Collection

The college collects personal data through the following methods:

a) Direct Collection
- Application and registration forms (online or physical);
- Employment recruitment processes;
- Student admission and enrolment systems;
- Academic and examination submissions;
- Surveys, consent forms and complaint forms;
- Face to face interactions with college staff;
- Questionnaires (research & Consultancies).

b) Automated or System-Based Collection
- Learning Management Systems (LMS);
- Student Information Management Systems (SIMS);
- Human Capital Management Information Systems (HCMIS);
- National e-Procurement System of Tanzania (NeST);
- Email systems;
- CCTV systems;
- Biometric attendance devices;
- Online portals and college websites.

c) Third-Party Sources

- MDA's and LGA's (e.g., NECTA,NIDA,PO PSM&GG,TAMISEMI, GSO);
- Sponsoring organizations;
- Previous institutions (academic transcripts or verification);
- Regulatory or accreditation bodies (TCU, NACTVET);
- Financial institutions (HESLB, Banks, SACCOs, etc);
- Employee Self Service (ESS) portal.

2.3. Data subject Rights

The college recognizes and upholds the rights of all individuals: students, staff, faculty, visitors and third parties whose personal data is collected or processed. These rights ensure transparency, fairness and accountability in the management of personal information.

2.3.1. Right to Be Informed

Individuals have the right to:

i. Be told what personal data is being collected;
ii. Understand why it is being collected and how it will be used;
iii. Know the legal basis for data processing;
iv. Be informed of data retention periods, data sharing, and their rights;

The college must provide clear and accessible privacy notices.

2.3.2. Right of Access

Individuals may request:

i. Confirmation of whether the college holds their personal data;
ii. Access to the data being processed;
iii. Information about processing purposes and categories of data;
iv. Details of third parties with whom the data is shared;

The College must respond within a reasonable timeframe.

2.3.3. Right to Rectification (Correction)

Individuals have the right to:

i. Request correction of inaccurate, outdated, or incomplete personal data;
ii. Have amended information updated in all relevant systems and records;

The college must ensure that corrections are made promptly.

2.3.4. Right to Erasure (Right to Be Forgotten)

Individuals may request deletion of their data when:

i. It is no longer necessary for the purpose collected;
ii. Consent is withdrawn and there is no other legal basis for processing;
iii. The data has been unlawfully processed;

This right is subject to exceptions, such as academic recordkeeping and legal obligations.

2.3.5. Right to Restrict Processing

Individuals may request the college to limit how their data is used when:

i. The accuracy of the data is disputed;
ii. Processing is unlawful but the individual prefers restriction over deletion;
iii. The college no longer needs the data but the individual requires it for legal claims.

Restricted data must not be processed further unless legally permitted.

2.3.6. Right to Data Portability

Individuals have the right to:

i. Receive their personal data in a structured, commonly used, machine-readable format;
ii. Request that the college transmit their data to another institution or organization, where technically feasible.

This right applies when data processing is based on consent or contract.

2.3.7. Right to Object

Individuals may object to:

i. Processing carried out based on legitimate interests or public interest;
ii. Use of personal data for marketing or non-academic communication;
iii. Certain forms of automated processing.

The college must stop processing unless it demonstrates compelling legitimate grounds.

2.3.8. Rights Related to Automated Decision-Making and Profiling

Individuals have the right to:

i. Not be subject to decisions made solely through automated processing that significantly affect them (e.g., automatic admissions decisions without human review);

ii. Request human intervention or contest automated decisions.

2.3.9. Right to Withdraw Consent

Individuals can withdraw consent at any time when processing is based on consent. Withdrawal must not affect the lawfulness of prior processing.

2.3.10. Right to Complain

Individuals have the right to:

i. Lodge data protection-related complaints to the College's Rector and Chief Executive Officer through Form Number 4 for the prevention of collection or processing of personal data; Form Number 5 for rectification of Persona Data and Form Number 6 for erasure or destruction of Personal Data.
ii. Escalate the complaint to the Personal Data Protection Commission (PDPC) of Tanzania if unsatisfied;
iii. Seek judicial remedies where applicable.

2.3.11. Right to Confidentiality and Data Security

Individuals are entitled to:

i. Expect that their personal data is kept confidential;
ii. Expect appropriate technical and organizational measures to prevent unauthorized access, loss or misuse.

2.4. Processing Sensitive Personal Data and/or Genetic or Biometric Data

Sensitive personal data including health information, disability status, ethnic origin, religious beliefs, genetic data and biometric identifiers is subject to enhanced protection due to its high-risk nature. The College shall implement the following procedures:

2.4.1. Lawful and Limited Collection

i. Sensitive data shall only be collected when strictly necessary for academic, administrative, legal or public interest purposes;
ii. Collection must have a clear legal basis, such as: Explicit consent from the individual; Compliance with statutory or regulatory requirements; Protection of vital interests (e.g., medical emergencies).

2.4.2. Explicit and Informed Consent

i. Individuals must provide written, explicit consent before the College collects or processes sensitive or biometric data, except where legally exempted;

ii. Consent forms must clearly state:(*Purpose of collection; Types of data being collected; How the data will be used and stored; Rights of the data subject; Retention periods*).

2.4.3. Strict Access Controls

i. Access to sensitive and biometric data shall be restricted to authorized personnel only;
ii. Access must follow: (*Role-based permissions; Need to know principles; Approval by the Data Protection Officer (DPO) or relevant authority*);
iii. Biometric data systems (e.g., fingerprint, facial recognition) must be secured with multi-layer authentication.

2.4.4. Secure Storage and Transmission

i. Sensitive data must be stored in encrypted databases or secure physical storage with restricted access;
ii. Any digital transmission must use: (*Encryption; Secure file transfer protocols; VPN or secure internal networks*);
iii. Hard-copy documents must be stored in locked cabinets within controlled access areas.

2.4.5. Data Minimization and Purpose Limitation

i. Only the minimum necessary amount of sensitive data shall be collected;
ii. Data shall not be used for purposes other than those originally stated unless new consent is obtained.

2.4.6. Special Handling of Biometric and Genetic Data

i. Biometric identifiers shall be processed only for: Access control; Time and attendance; Examination integrity verification; Security operations;
ii. Genetic data shall be processed only when required by law, research protocols, or medical fitness assessments and must undergo ethics approval.

2.4.7. Privacy Impact Assessments (PIA)

Before introducing biometric systems, health data systems, or research involving genetic data, a Data Protection Impact Assessment (DPIA) must be conducted to: Assess risks; Determine safeguards; and justify the processing's necessity and proportionality.

2.4.8. Confidentiality Agreements

i. All staff handling sensitive data must sign confidentiality agreements and undergo data protection training;
ii. Breaches of confidentiality shall result in disciplinary action.

2.4.9. Limited Retention and Secure Disposal

i. Sensitive data shall be retained only for the period required by law or institutional need. " *refer to college records retention and disposal schedule*";
ii. Secure disposal methods include: Digital deletion with overwrite methods; Shredding of paper documents; Deactivation and purging of biometric templates.

2.4.10. Incident Management and Breach Reporting

i. Any suspected or actual breach of sensitive or biometric data must be immediately reported to the Rector and Chief Executive Officer;
ii. The college shall: investigate the incident promptly; notify affected individuals as required; and take corrective and preventive actions.

2.4.11. Regular Compliance Monitoring

i. The College shall conduct periodic internal audits and reviews of systems processing sensitive data.
ii. Biometric and genetic data processing shall be monitored to ensure Compliance with the Personal Data Protection Act No. 11 of 2022; Adherence to ethical standards of research and academia.

2.5. Consent Management

The college is committed to ensuring that all processing of personal data based on consent is conducted lawfully, transparently, and in accordance with applicable data protection regulations. The following procedures outline how consent shall be obtained, managed, stored and withdrawn.

2.5.1. Obtaining Consent

a) Clear and Informed Consent
   i. Consent must be obtained through a clear, understandable statement provided to the individual before data collection.
   ii. Individuals must be informed of the purpose of data collection; the type of data being collected; how the data will be used, stored, and shared; their right to withdraw consent at any time; the consequences of refusing or withdrawing consent.

b) Explicit Consent for Sensitive Data

For sensitive personal data (e.g., health, biometric, genetic, disability related information), explicit written consent is required unless a legal exemption applies.

c) Voluntary and Unforced
Consent must be freely given, without enforcement, pressure, or making services conditional unless the data is strictly necessary for service delivery.

d) Age and Capacity Checks
For minors or individuals lacking legal capacity, consent must be obtained from a parent, guardian, or authorized representative.

2.5.2. Managing Consent

a) Consent Tracking Systems
All consent records must be stored in a secure digital or physical system that allows tracking of: who gave the consent; when it was given; the specific purpose for which it was obtained; the method used to provide the consent.

b) Review and Renewal
i. Consent for long-term or ongoing processing (e.g., student records, research participation) must be reviewed periodically.
ii. Renewal of consent is required if: the purpose of processing changes; new data categories are added; legal obligations evolve.

c) Limited Scope
i. Consent must be used only for the specific purpose for which it was provided.
ii. Any additional processing requires new consent.

d) Documenting Consent
i. Record keeping Requirements
The college must maintain documented proof of consent, including: Signed consent forms (paper or electronic); Timestamped digital confirmations; Email or system-based acknowledgments; Logs from online platforms (e.g., LMS, application portals).

ii. Secure Storage
Consent records must be stored securely, accessible only to authorized personnel. Storage systems must ensure: Confidentiality; Integrity; Availability of consent information when required.

e) Auditability
Consent documentation must be retained in a form that allows internal and external audits to verify compliance.

2.5.3. Withdrawing Consent

a) Right to Withdraw

Individuals may withdraw consent at any time without negative consequences, except where the data is required for: legal compliance, contractual obligations, public interest functions.

b) Simple Withdrawal Process

The college shall provide clear and accessible ways for individuals to withdraw consent, such as: Email to the DPO, Online forms, Written requests, Opt-out buttons on digital systems.

c) Timely Action

Upon withdrawal, the college must: Stop processing the affected data; update systems and records; notify relevant departments, units or section; confirm withdrawal to the individual.

d) Retention After Withdrawal

Data processed before consent withdrawal remains lawful, but further processing shall cease unless another legal basis applies.

e) Staff Responsibilities

i. All staff involved in data collection must be trained on consent procedures.
ii. Departments/section or Units must use only approved consent forms and templates.
iii. The Data Protection Officer (DPO) oversees compliance and provides guidance.

f) Monitoring and Compliance

i. Regular audits will be conducted to ensure adherence to consent procedures.
ii. Non-compliance will result in corrective action, including staff training, disciplinary measures, or system improvements.

2.6. Data Security and Storage

The college is committed to ensuring the integrity, confidentiality and availability of all personal data under its control. To achieve this, the college implements robust technical, physical and administrative safeguards designed to prevent unauthorized access, loss, alteration or misuse of personal information. These measures apply to all forms of data digital, physical, archived and active records.

2.6.1. Commitment to Robust Security Measures

i. Protection of Data Integrity

- The College ensures that personal data is accurate, complete and protected from unauthorized modification.

- Systems handling personal data are monitored to detect and prevent corruption or tampering.
- Secure backup routines are implemented to maintain data consistency in the event of system failure.

ii. Protection of Data Confidentiality

- Access to personal data is restricted based on the need-to-know principle and role based permissions.
- Strong authentication mechanisms (password policies, two factor authentication, biometrics) are enforced.
- Data is encrypted both during transmission and storage.
- Staff handling personal data must sign confidentiality agreements and undergo regular training.

iii. Ensuring Data Availability

- Systems storing personal data are designed to remain accessible for authorized use while protected against cyber threats and operational disruptions.
- The College implements: Regular system maintenance; High-availability infrastructure; Business continuity plans; and Disaster recovery solutions.

2.6.2. Secure Data Storage Practices

a) Digital Storage

i. Personal data is stored in secure servers, cloud systems approved by the ICT Unit or institutional data centers.
ii. Security controls include: Encryption at rest; Firewalls and intrusion detection systems; Access logs and audit trails; Regular security patching and updates.

b) Physical Storage

i. Hard-copy documents containing personal data are stored in: Locked cabinets; access-controlled rooms; archives with restricted entry.
ii. Only authorized personnel may retrieve or handle these documents.

c) Backup and Recovery

i. Backups are conducted regularly and stored in secure on-site and/or off-site locations.
ii. Backup integrity is tested periodically to ensure accessibility and accuracy.

iii. The Disaster Recovery Plan (DRP) ensures rapid restoration of critical systems.

d) Secure Disposal

i. Data that has reached the end of its retention period is disposed of securely using approved methods: Shredding of paper records; secure wiping or degaussing of digital media; permanent deletion from active systems.

ii. Disposal activities must be documented and supervised to prevent data leakage.

2.6.3. Monitoring, Compliance, and Continuous Improvement

i. The college conducts regular security assessments, audits and vulnerability scans.

ii. The ICT unit and Data Protection Officer (DPO) monitor compliance with security policies and legal obligations.

iii. Security practices are continuously reviewed and updated to address emerging risks, new technologies, and regulatory changes.

iv. Any actual or suspected security breach must be reported immediately and managed according to the college's Incident Response Procedures.

2.6.4. Responsibilities of Staff and System Users

i. All personnel must adhere to established data security protocols.

ii. Users are responsible for safeguarding passwords, reporting suspicious activity, and following safe handling procedures for personal data.

iii. Departments/ units/sections must store data only in approved systems and avoid unauthorized applications or personal devices.

2.7. Complaints Handling

The College is committed to ensuring that all individuals have the right to raise concerns regarding the handling of their personal data. The following procedures outline how complaints or request related to data protection shall be received, assessed, investigated, and resolved in a fair, transparent and timely manner.

Procedures for Managing and Resolving Personal Data Protection Complaints

2.7.1. Procedures of enforcing Rights of Data Subjects

When a data subject desires to invoke their rights in regard to any of their personal data that the College processes, they should do so through a process set out as follows:

a) Prevention of collection or processing of personal data

In cases where collection or processing of personal data is likely to cause significant harm to the data subject or any other person, the data subject can ask the College not to proceed or suspend processing of the said data.

Such request will be made through use of Form Number 4 provided in First Schedule to Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.

b) Procedure for rectification of personal data

A data subject is allowed to make request for the correction of personal data which could be incomplete, incorrect, misleading, outdated, or has since changed.

The above request should be made using Form Number 5 in the First Schedule to Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.

It may also be accompanied by documentation that will help in correction of the personal data concerned.

c) Procedure for erasure or destruction of personal data

The data subject is entitled to request from the College that the personal data collected be destroyed or erased from its records. The data subject shall be able to make such an application requesting the destruction or erasure of his personal data in Form No. 6 annexed in the First Schedule to Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.

2.7.2. Acknowledgement of Receipt

Upon receiving a complaint, the Data Protection Officer shall:

i. Acknowledge receipt in writing within a specified timeframe (3 working days);
ii. Provide a reference number for tracking;
iii. Outline the next steps and expected timeframes for resolution.

2.7.3. Preliminary Assessment

The DPO shall conduct an initial review to:

i. Determine whether the complaint relates to personal data protection;

ii. Assess the urgency and severity of the matter (e.g., potential data breach, unauthorized disclosure, denial of rights);
iii. Identify which departments or officers should be involved; and
iv. If the complaint falls outside the DPO's mandate, the individual will be guided on the appropriate office or procedure.

2.7.4. Investigation Procedure

The Data Protection Officer shall carry out a formal investigation, which may include:

i. Reviewing system logs, records, or relevant files;
ii. Interviewing staff or individuals involved in the incident;
iii. Consulting ICT, HR, legal, or administrative units as necessary;
iv. Assessing compliance with internal policies and legal requirements.

All investigations must be conducted objectively, confidentially, and without bias.

2.7.5. Resolution and Corrective Actions

Based on the investigation findings, the college shall:

i. Provide a written response to the complainant outlining the outcome;
ii. Implement corrective measures where violations are identified, *such as: (Updating or correcting personal data; Restricting or halting improper data processing; Strengthening internal controls or training; Disciplinary action against staff / student, where applicable;)*
iii. Notify the complainant of steps taken to resolve the matter.

Where the complaint involves a data breach, appropriate incident response protocols shall apply.

2.7.6. Right to Appeal or Escalate

If the complainant is dissatisfied with the outcome, they may:

i. Escalate the complaint to the Personal Data Protection Commision;
ii. Seek legal remedies as permitted by law.

The college must provide guidance on how to escalate unresolved concerns.

2.7.7. Recordkeeping and Documentation

The college shall maintain secure records of:

i. All complaints received;
ii. Actions taken;
iii. Investigation reports;
iv. Resolutions provided.

These records support transparency, institutional learning and compliance auditing.

2.7.8. Continuous Improvement

Complaints shall be reviewed periodically to:

i. Identify recurring issues;
ii. Strengthen policies and operational controls;
iii. Improve staff awareness and training.

2.8. Roles and Responsibilities of a Data Protection Officer (DPO)

Pursuant to the Personal Data Protection Act (Cap. 44) and the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 (Regulation No. 32), a Data Protection Officer shall have the following duties:

(a) to ensure compliance with the Act and these Regulations in the processing of personal data carried out by the data controller or data processor;
(b) to provide information on violations of the provisions of the Act or these Regulations committed in the processing by the data controller or data processor and advise rectification measures;
(c) to prepare and submit quarterly reports on the compliance of the Act to the Commission;
(d) handling the applications or complaints made by the data subject, his representative or another person to the data controller or data processor in relation to the collection or processing of personal data; and
(e) to perform any other duty as may be directed by the data controller or data processor.

2.9. Employees Training and Awareness

The College shall ensure that all staff, students, contractors, and affiliated institutions handling Personal Data understand and comply with this Policy. Continuous awareness, training, and monitoring shall be undertaken to promote a culture of privacy, accountability and ethical data governance across all College functions.

The College leadership affirms its full commitment to enforcing this Policy and ensuring that all Personal Data is managed with integrity, respect and due diligence, thereby maintaining the trust and confidence of all stakeholders.

2.10. Data Retention and Disposal

The college discourages the retention of Personal Data for longer than it is required. Considerable amounts of data are collected about staff, students, applicants, research subjects, etc. However, once a member of staff or student has left the college or the purpose for which that data was collected has ended, it will not be necessary to retain all the information held on them. Some Personal Data will be kept for longer periods than others. The college's Records Retention and Disposal Schedule (RRDS) should be followed for the retention and disposal of Personal Data.
The college aims to reduce the duplication of personal data and will encourage as far as possible the use of definitive central sources of information for data used across the college (e.g. contact addresses). Those with legitimate reason will have access to the Personal Data relevant for their job. Permissions granted for such access will be logged where possible and regularly reviewed.

The creation of systems and/or files which duplicate such data should be avoided; where it is inevitable every care should be taken to ensure that data maintained in subsidiary systems is fully synchronised with definitive sources, and updated frequently through secure and reliable interconnection.

(a) Students
In general, electronic student records maintained in the college's Applicant and Student Information Management System (SIMS) are kept permanently in order to fulfil the requirement for the provision of transcripts during a student's or former student's working life. Such information would typically include name and address on entry and completion, programmes taken, examination results and awards obtained. Departments should regularly review the personal files that they hold relating to individual students (whether stored electronically or in paper records) in accordance with the college's Records Retention and Disposal Schedule.

(b) Staff
In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by Human Resources for 10 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay, etc. will be retained for the statutory time period (5 years).

Staff personnel records are kept and maintained by Human Resources unit. Other departments should only keep staff information where necessary for legitimate business purposes. To the extent that files of individual staff members are kept outside Human Resources, unit should regularly review those files in accordance with the college's Records Retention and Disposal Schedule.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date and should then be securely destroyed as confidential waste. Human Resources may keep a record of names of individuals that have applied, been shortlisted, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

(c) Disposal of Records

Personal Data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with the college's Retention and Disposal Schedule.

NB: ***All matters relating to the retention and disposal of Personal Data shall be governed strictly in accordance with the College's official records retention and disposal schedule***.

2.11. Personal Data Breach Notification

Staff and students are trained to recognize potential personal data breaches, including unauthorized access, loss or accidental disclosure of personal information. Monitoring systems, such as access logs and IT security alerts, are in place to detect unusual activity that may indicate a breach. Any suspicion of a breach is taken seriously, regardless of its perceived severity.

All staff and students are required to immediately report suspected or confirmed breaches to the designated Data Protection Officer (DPO). A standard reporting procedure ensures that all relevant details such as who was involved, what occurred, when it happened and how it happened are properly documented. Timely reporting is essential to minimize risks and maintain compliance with data protection regulations.

Once a breach is reported, the DPO or responsible team investigates to assess its severity and potential impact. Containment and mitigation measures are implemented promptly to prevent further data loss or unauthorized access. Affected individuals are notified if required by law, and remedial actions, such as updating security protocols or providing staff

guidance, are taken. Each breach is recorded, lessons learned are documented, and procedures are reviewed to prevent similar incidents in the future.

2.7.1. Personal Data in the Public Domain

The College holds certain information about staff and students in the public domain like for example on the college web site or in publications. Personal data classified as being in the ‘public domain’ refers to information that is already publicly available and may be disclosed to third parties without having to seek consent from the data subject.

The college will make some personal data publicly available unless individuals have objected, like for example: names, workplace email addresses, telephone numbers, academic qualifications, biographies and curricula vitae of academic staff, support staff, Committee members and MAB members where supplied and where appropriate.

The college may process personal information about third parties which is already in the public domain where such processing is carried out in accordance with the Personal Data Protection Act principles and is unlikely to cause any damage or distress to the data subject.

2.12. Privacy Notes

The college shall issue privacy notices in respect of its processing of Personal Data of students, staff, alumni, certain partners and visitors, which tell those people what data is collected about them, what it is used for, the legal basis for Processing the data, who it will be shared with and how long it will be held for. When collecting Personal Data or introducing new data protection activities, members of staff must consider existing privacy notices to determine whether they are to be refreshed to take account of the new activities, or whether new privacy notices are required to cover that activity. They must also ensure that any new Processing activities are added to the college's Record of Processing Activities.

There are very limited exceptions to providing notice to Data Subjects of activities constituting processing. In any case of doubt as to whether notice should be provided or updated, staff must consult their Data Protection Officer.

If staff or students Process Personal Data on behalf of another party then due diligence must be undertaken and contractual protection sought to ensure the other party has provided/received adequate data protection notices or consents.

2.13. Data Protection Impact Assessments (DPIAs)

The institution performs Data Protection Impact Assessments (DPIAs) on all its data processing operations to ensure that the operations are Data Protection compliant and do not pose risks to individuals' personal data. This assessment takes place before embarking on any project or process that involves the collection, use, or disclosure of personal data, especially when the risks to individuals' privacy are significant.

It involves determining the type of data to process, risks to the subjects, and mechanisms to reduce these risks. Results of a DPIA are documented, and where necessary, modifications to the process of collecting the information take place before carrying out data collection. The Data Protection Officer helps in the process, and DPIAs undergo regular scrutiny to check compliance.

2.14. Transborder Flow of Personal Data

2.14.1. Transfers to Third Parties

The College shall only reveal personal data to, or permit third party access to, third parties (including Cloud Computing services) if it can be ensured that the personal data will be processed lawfully and sufficiently safeguarded by the third party. Third party processing of personal data may occur, and prior to this, the College shall determine if, under the relevant laws, the third party is a data controller or data processor of the personal data.

In cases where the Third Party is considered to be a data controller, the college shall agree an appropriate agreement with the Controller regarding their respective obligations with respect to the processed personal data through an Information Sharing Agreement.

In the case where the Third Party is considered the data processor, the college shall then establish an adequate contract of processing with the said data processor in the form of Data Sharing Agreement in order to ensure that the latter uses appropriate measures in protecting the personal data.

The college shall carry out regular audits of the personal data processing carried out by third parties, in particular in relation to the technical and organisational measures that they have established. Any significant deficiencies will be reported to and will be monitored by the college.

2.14.2. Data Transfers to another Country

A data controller or data processor who intends to transfer personal data outside the country, shall submit an application for permit to the Commission using Form No. 7 set out in the First Schedule to "*Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023*"

The Commission is required to consider any application submitted within fourteen days of receipt, in accordance with the provisions of the Personal Data Protection Act and Regulations. After reviewing the application, the Commission may either accept or reject it. If the application is accepted, the Commission will issue a permit to transfer personal data using Form No. 8, as set out in the First Schedule to the Regulations. In cases where the application is rejected, the Commission must notify the applicant in writing and provide the reasons for the rejection.

2.15. Sharing Personal Data

Personal information shall only be shared for the relevant purpose and in line with the requirements of the Personal Data Protection Act, Tanzania, and other relevant laws. The information is shared with the concerned individuals, and consent is sought when it is necessary. Where data is shared with third parties, it is in line with the signed agreement involving the purpose, mechanism for securing the information, use, and obligations of the third parties. Data is shared with authorized persons, and the volume shared is restricted to the required level. All data is shared, and the process is reviewed.

2.16. Disclosure of Personal Data

The college is responsible for ensuring that the Personal Data is not revealed to unauthorized third parties. This would include family and friends, government departments, the Press, and in some cases, the Police.

It is important that all staff and students be very cautious when asked to provide Personal Data held by the college about another person to a third party. For example, it would be taken as acceptable to provide the work contact information of a colleague when asked for information about a particular function they are responsible for.

However, it would not normally be appropriate to provide personal information about a colleague to an individual seeking to make contact with them in connection with a matter outside of their role at the college, particularly where that personal information is not otherwise public (for example, their work

contact information on the college's web site). The crucial aspect to keep in mind is the relevancy and necessity of the information for purposes of conducting the business of the college.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

a) where the disclosure is in the legitimate interests of the college (*e.g. disclosure to staff – Personal Data can be disclosed to other college employees if it is clear that those members of staff require the information to enable them to perform their jobs*);
b) where disclosure of data is required for the performance of a contract (e.g. informing Student sponsor of course changes /withdrawal, etc.).
c) If Personal Data is to be shared with a third party in connection with the performance of a contract, then approved data protection clauses must be included in the relevant contract. The college Data Protection Officer should be consulted on every occasion before any such contracts are entered into and Personal Data must not be shared with the third party until an appropriate contract is in place.
d) The Data Protection Laws permit certain disclosures without notification to the Data Subject in certain cases, so long as the information is requested for one or more of the following purposes:
    i. to safeguard national security;
    ii. prevention or detection of crime including the apprehension or prosecution of offenders;
    iii. assessment or collection of tax duty of fee;
    iv. discharge of regulatory functions (includes health, safety and welfare of persons at work);
    v. to prevent serious harm to a third party; or
    vi. to protect the vital interests of the individual; this refers to life and death situations.
e) Requests must be supported by appropriate paperwork and should follow the agreed protocols if in place. Where a third-party request is received citing one of these grounds, the request should be passed to an authorised person within the college for approval before any information is related. The authorised personnel are, the Data Protection Officer, the Rector/CEO, the Deputy Rector and respective Directors.
f) When members of staff receive enquiries as to whether a named individual is a member of the college (staff or student), the enquirer should be asked why the information is required. If consent for disclosure has not

been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment.

g) Unless the Data Subject has requested otherwise, Personal Data should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing Personal Data, the college may offer to do one of the following:

i. pass a message to the Data Subject asking them to contact the enquirer; or
ii. accept a sealed envelope/incoming email message and attempt to forward it to the Data Subject.

Inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the college" to avoid confirming their membership of, their presence in or their absence from the institution. If in doubt, staff should seek advice from their Supervisor or Data Protection Officer.

2.17. Use of CCTV

The installation and use of CCTV and surveillance technologies are also expected to be in line with the Personal Data Protection Act in the country of Tanzania and all the applicable legislation. CCTV and surveillance technology shall only be used for legal purposes, and this includes personal and institutional security. Only authorized personnel, the ICT officer and Human Resources Management and Administration staff are authorized to use the technology. Personal data subject to surveillance shall be identifiable, with the minimum collected necessary, safely stored, and not held for longer than necessary as per the college's RRDS, and all personal data shall be safely and securely destroyed. There shall be confidentiality by the staff operating the surveillance technology.

2.18. Cookies and Online Tracking

The use of cookies and tracking mechanisms needs to be done in line with the Personal Data Protection Act, among others. The use of the cookie and online tracking mechanisms shall be for legitimate purposes, such as optimizing the functionality of the sites, offering better user experience, and

understanding how the sites are used. Users shall be informed about the privacy notice and consent shall be obtained where necessary, apart from those that are non-essential. Data shall be collected and anonymized where possible, and shall be accessible only to those who are authorized. Personal data collected through the use of the cookie shall be held for as long as is necessary and disposed of in compliance with the Retention and Disposal Schedule.

2.19. Online Privacy Rights for Special Groups

Special groups, including children, vulnerable individuals, and those with specific needs, require enhanced protections for their online privacy in compliance with the Personal Data Protection Act of Tanzania and other relevant regulations. Explicit consent must be obtained from parents or guardians before collecting or processing children's personal data. Information about data collection, usage, and rights must be communicated in clear, accessible language. Only the minimum necessary data should be collected, and additional technical and organizational measures must be implemented to secure it.

2.20. Data Protection by Design and by Default

To identify all requirements in the area of data protection while developing a new system or process or while re-examining existing ones, all of them need to follow the approval process in order to proceed.
Each department has to ensure that a Data Protection Impact Assessment (DPIA) takes place, in association with the Data Protection Officer, with regard to all new and/or amended systems or processes that fall within its remit.
The outcome of the DPIA should then be submitted for review and approval by the Management.

2.21. Publication of College Information

The college publishes a number of items that include Personal Data, and will continue to do so. These are:

a) names of all members of college Committees (including Ministerial Advisory Board);
b) Academic staff profiles on the college website, including names, job titles and academic and/or professional qualifications and photographs;

c) Awards and Honours (including Honorary Graduands and other Honorary award recipients);
d) Staff Telephone and Email Directory;
e) Graduation programmes and videos or other multimedia versions of graduation ceremonies;
f) Information in prospectuses (including photographs), annual reports, staff newsletters, etc.;
g) Publicity information included in public relations stories and press releases and on social media; and
h) Staff information on the college website (including photographs).

It is recognized that there might be occasions when a member of staff, a student, or other party, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the college should use its reasonable endeavours to comply with the request and ensure that appropriate action is taken.

2.21.1. Academic Research

Personal Data collected only for the purposes of academic research (including work of staff and students) must be processed in compliance with the Data Protection Laws and in compliance with the college's Research Policy, Agenda and Strategy. The College will publish additional guidance to assist researchers in complying with these requirements.
Individual students or staff carrying out research should note that Personal Data may be processed for research purposes on the legal basis that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the college. Researchers may also rely on the bases that the processing is necessary for scientific or historical research purposes, or that it is necessary for statistical purposes.

Where the legal bases for Processing Personal Data referred to above are available to researchers, the consent of the Data Subject is not required. However, such processing is subject to safeguards to ensure that data is minimized (including being pseudonymised and anonymised) and that:

i. the Personal Data are not processed to support measures or decisions with respect to particular individuals; and

ii. the Data Subjects must not be caused substantial damage or substantial distress by the Processing of the Personal Data.
iii. If the above conditions are met, together with technical and organizational safeguards to keep data secure, Personal Data Processed for research purposes may be:
iv. Processed for purposes other than that for which it was originally obtained, including statistical or historical purposes; and
v. exempt from the Data Subject's right of access and rectification, as well as their right to restrict or object to Processing.

Other than this, Data Protection Laws apply in full in respect of academic research. The obligations to collect only necessary and accurate Personal Data, to hold Personal Data securely and confidentially and not to disclose Personal Data except in accordance with the Data Protection Laws (including in relation to publication) must all still be complied with.

2.21.2. Publication

Researchers should ensure that the results of research are anonymised when published and that no information is published that would allow individuals to be identified (including where anonymised data could be matched with other data to link back to an identifiable individual) where consent has not been obtained for such use from the Data Subject or, where the nature of the research makes it impracticable or otherwise undesirable to attempt to seek/obtain consent, that there is a legitimate interest in publication and publication would not unfairly damage the rights and freedoms of the Data Subject.

3. IMPLEMENTATION PROCEDURES, MONITORING AND EVALUATION

3.1. Implementation and Reviews

i. This document shall come into operation once tabled and agreed in a management meeting, approved by TPSC Ministerial Advisory Body (MAB) and finally approved by Personal Data Protection Commision.
ii. TPSC's management will use this document in conjunction with the Personal Data Protection Act and Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.
iii. All staff, students and other stakeholders of TPSC shall comply with requirements in this document.

3.2. Review

This document shall be reviewed within three years, or whenever the business environment of TPSC changes in a way that affects this current document.

3.3. Enforcement/ Disciplinary /Consequences for Policy Violations by TPSC Staff

TPSC staff found to have violated this policy may be subject to withdrawal and or suspension of systems and network privileges or disciplinary action in accordance with Public Service Act and Regulations.

Appendices

a) Forms extracted from the the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.

i. Prevention of collection or processing of personal “Form No. 4”

ii. Procedure for rectification of personal data “Form No. 5”

iii. Procedure for erasure or destruction of personal data “Form No. 6”

iv. Personal data transfer permit to the Commission “Form No. 7”

v. Permit to transfer personal data “Form No. 8”

b) College Forms

i. Breach Notification “Form No.1”

ii. Data Collection and Processing Consent “Form No. 2”

FORM NO.4

APPLICATION TO PREVENT COLLECTION OR PROCESSING OF PERSONAL DATA

(Made under regulation 15(2))

NOTE:

(i) *Documentary evidence substantiating the suspension or not to begin may be required.*

(ii) *If a space provided in this Form is not sufficient, submit the information as an appendix*

A. APPLICATION BASIS

Mark the appropriate box with a tick (✓):

SUSPENSION ☐ NOT TO BEGIN ☐

B. PARTICULARS OF DATA SUBJECT

Name: .....

Identification Number: .....

Phone number: .....

E-mail: .....

(State below if the data subject is a child or a person with disability)

Name: .....

Relationship with the Applicant: .....

Contact: .....

C. REASONS FOR THE APPLICATION

(Please provide detailed reasons for the application for suspension or not to begin the processing)

……

……

……

D. DECLARATION

I certify that the statements I made in this application are true

Date _____ Signature _____

FORM NO.5

(Made under regulation 16(1))

APPLICATION FOR RECTIFICATION OF PERSONAL DATA

Note:

(i) Any documentary evidence in support of the application may be attached.
(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure to this Form.
*(iii) All parts marked * are mandatory.*

A: PARTICULARS OF THE DATA SUBJECT

(This Part is for details of Data Subject)

Name*: ……

Identification Number*: .....

Phone number*: .....

E-mail: .....

(State below if the data subject is a child or a person with disability)

Name: .....

Relationship with the Applicant: .....

Contact: .....

Sign …….. Date …….

PROPOSED RECTIFICATION (S)

	Personal data currently to be rectified Name, physical address, mobile number, etc.	*The proposed rectification*	*Reason for the proposed rectification*
1.			
2.			
3.			

B: DECLARATION

I certify that I have read and understood the terms of this Form and confirm that the information given in this application is true.

(Please note that any attempt to gain access to personal data through misrepresentation may result in prosecution.)

Signature ……. Date ……..

FORM NO.6

(Made under regulation 17(2))

APPLICATION FORM FOR ERASURE

Fill as appropriate

Note:

(i) Any documentary evidence in support of the application may be attached.

(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure to this Form.

*(iii) All parts marked * are mandatory.*

i. PARTICULARS OF DATA SUBJECT

(This Part is for details of Data Subject)

Name*: ……

Identification Number*: .....

Phone number*: .....

E-mail:.....

(State below if the data subject is a child or a person with disability)

Name: .....

Relationship with the Applicant: .....

Contact: .....

ii. REASONS FOR ERASURE OF PERSONAL DATA

(Mark the appropriate box with a tick (✓))

Specify the reason(s) for which you want the personal data to be erased.

(a) The personal data is no longer necessary for the purposes for which was originally collected	
(b) You have withdrawn the consent that was the legal basis for the storage of personal data;	
(c) You are objecting to the processing of your personal data and there is no legal interest to proceed with the processing;	
(d) Your personal data has been unlawfully processed;	
(e) You are required to fulfil legal obligations.	

iii. DECLARATION

I confirm that I have read and understood the terms of this application form and certify that the information given in this application is true.

(Please note that any attempt to gain access to personal data through misrepresentation may result in prosecution.)

Signature: ..... Date: .....

FORM NO.7

(Made under regulation 20(1))

APPLICATION FORM FOR PERMIT TO TRANSFER PERSONAL DATA OUTSIDE THE COUNTRY

I. PARTICULARS OF THE APPLICANT

Name.....

Identification Number ……

Data Controller /Data Processor……

Physical Address ……..……

Postal Address ……..……..

Phone Number: .....

Email Address: .....

II. PARTICULARS OF THE RECIPIENT

Name.....

Identification Number ……

Data Controller /Data Processor……

The Country of the Recipient ……..……

Physical Address ……..……

Postal Address ……..……..

Phone Number: .....

Email Address: .....

III. PARTICULARS OF THE DATA SUBJECT

Name .....

Citizenship ……

Age ……..……

Gender ……..….

Identification Number …….

Phone Number: .....

Email Address: .....

(State below if the data subject is a child or a person with disability)

Name .....

Citizenship ……

Age ……..……

Gender ……..….
Identification Number …….
Relationship with the Applicant: .....
Contact: .....
I certify that the information provided in this application are true.

IV. THE CATEGORY OF THE PERSONAL DATA TO BE TRANSFERRED

……

……

V. THE PURPOSE AND NECESSITY OF TRANSFER THE PERSONAL DATA

……

……

VI. STATEMENT OF SECURITY OF PERSONAL DATA IN THE COUNTRY OF RECEIVER:

(Mark with a tick on the appropriate information)

i. The country you are requesting to transfer personal data has a Personal Data Protection Law;
ii. A country receiving personal data has ratified the International Convention making provisions in relation to the protection of personal data;
iii. There is an agreement between the United Republic and the country that receives data on the protection of personal data; or
iv. There is a contractual agreement between the data applicant and the person receiving the personal data who is outside the country.

VII. DATE AND TIME OF TRANSFER OF PERSONAL DATA:

……./……../……

VIII. ANY OTHER INFORMATION NEEDED BY THE COMMISSION

……

……..……

IX. CONSENT OF DATA SUBJECT:
I consent to my personal data being transferred outside the country as provided in this form.

SIGNATURE OF THE DATA SUBJECT DATE

…… ……/…….20……

SIGNATURE OF THE APPLICANT DATE

…… ……/……20……

FORM NO. 8

(Made under regulation 20(6))

PERMIT NUMBER ….....

A PERMIT TO TRANSFER PERSONAL DATA OUTSIDE THE COUNTRY

The Commission after considering the application submitted by the applicant and subject to the provisions of the Personal Data Protection Act and its Regulations has accepted the application of .....……, the Applicant (Data Controller/Data Processor), of transferring the personal data of ……..… *(Data Subject),* to ……...…., the Recipient of ……. *(Country),* on the ……. / 20…… *(date)*

The Commission has therefore approved that the Data Controller/Data Processor mentioned in this Permit may transfer Personal Data out of the country as requested in accordance with sections 31 and 32 of the Personal Data Protection Act, No.11/2022.

GIVEN with the stamp of the COMMISSION this …….... day of ……20……..

DIRECTOR GENERAL OF THE COMMISSION

TANZANIA PUBLIC SERVICE COLLEGE (TPSC)

FORM No.1

DATA COLLECTION AND PROCESSING CONSENT FORM

1. PURPOSE OF DATA COLLECTION

The College collects personal data for the following purposes:

_____

_____

_____

2. TYPES OF DATA COLLECTED

The College may collect the following categories of personal data:
☐ Personal Identification Data
☐ Contact Information
☐ Academic Records
☐ Financial Information
☐ Health Information (if applicable)
☐ Other (specify): _____

3. USE OF DATA

Your personal data will be used for:

_____

_____

4. DATA STORAGE AND SECURITY

Data will be stored in: ☐ Electronic form ☐ Physical records ☐ Both

Security measures in place include:

_____

_____

5. DATA SUBJECT RIGHTS

You have the right to:
☐ Access your data
☐ Request correction of your data
☐ Request deletion of your data (where applicable)
☐ Restrict or object to processing
☐ Withdraw consent

Additional notes:

6. DATA RETENTION PERIOD

Your personal data will be retained for:

After this period, the data will be:
☐ Deleted ☐ Archived ☐ Anonymized

7. CONSENT DECLARATION

I confirm that I have been informed about the collection and use of my personal data and I give my consent as described above.

8. DATA SUBJECT DETAILS

Full Name: _____

ID/Registration Number: _____

Contact Information: _____

Signature: _____

Date: _____

9. FOR MINORS (IF APPLICABLE)

Parent/Guardian Name: _____

Signature: _____

Date: _____

10. FOR OFFICIAL USE ONLY

Received By: _____

Position: _____

Signature: _____

Date: _____

FORM No. 2

PERSONAL DATA BREACH NOTIFICATION FORM

TPSC PERSONAL DATA BREACH NOTIFICATION FORM

1. REPORT DETAILS

Report Reference Number: _____

Date of Report: _____

Time of Report: _____

2. REPORTER INFORMATION

Full Name: _____

Role (Staff/Student): _____

Department/Course: _____

Contact Information (Phone/Email): _____

3. BREACH IDENTIFICATION

Type of Report:
☐ Suspected Breach
☐ Confirmed Breach

Date Breach Occurred (if known): _____

Time Breach Occurred (if known): _____

Date Breach Discovered: _____

Time Breach Discovered: _____

4. INCIDENT DESCRIPTION

(Provide a clear and detailed explanation of what happened)

5. PERSONAL DATA INVOLVED

Type of Data:
☐ Personal Identification Data
☐ Academic Records
☐ Financial Information

☐ Health Information
☐ Other (specify): _____

Approximate Number of Individuals Affected:
_____

6. CAUSE OF BREACH

(Explain how the breach occurred)

_____

_____

7. PERSONS / SYSTEMS INVOLVED

(Provide details if known)

_____

_____

_____

8. DETECTION METHOD

How was the breach identified?
☐ Access Logs
☐ IT Security Alert
☐ Reported by Individual
☐ Other (specify): _____

9. IMMEDIATE ACTION TAKEN

(Describe any steps already taken to contain or reduce the breach)

_____

_____

10. RISK & IMPACT ASSESSMENT (For Official Use Only)

Severity Level:
☐ Low
☐ Medium
☐ High

Potential Impact:

_____

_____

11. NOTIFICATION & RESPONSE

Were affected individuals notified?
☐ Yes ☐ No

If yes, Date of Notification: _____
Mitigation Actions Taken:

12. INVESTIGATION OUTCOME *(For Official Use Only)*

Findings:

Root Cause:

13. CORRECTIVE & PREVENTIVE ACTIONS

Actions Taken:

Recommendations:

14. CLOSURE DETAILS

Date Case Closed**:** _____

Closed By (Name & Title): _____

Signature: _____

15. LESSONS LEARNED