UNIVERSAL TECHNOLOGY AND MANAGEMENT UNIVERSITY

UTAMU

For an Open Mind

UTAMU DATA PROTECTION AND PRIVACY POLICY, 2026.

APPROVAL

This Policy was formulated and recommended by the University Management and is hereby approved by the University Council of Universal Technology and Management University (UTAMU).

Table of Contents

1.0 INTRODUCTION

1.1 Background

Universal Technology and Management University (UTAMU) was granted a provisional license by the National Council for Higher Education (NCHE) on 11 March 2013 (License No. UIPL022), and its name and particulars were published in the Uganda Gazette Vol. CVI No. 14 of 22nd March 2013 under Legal Notice No.4 of 2013.This Policy operationalises UTAMU's Vision, Mission and Core Values by embedding lawful, ethical and transparent data governance practices across the University.

The Vision of UTAMU is A global educational institution of excellence in management, science, technology and innovation whereas the mission is to provide global quality education, research and innovation critical to economic and human development. The core values of the University are professionalism, creativity, integrity, transparency, empowerment and community engagement.

1.2. Institutional Alignment

This Policy supports UTAMU's Vision of global excellence and its Mission of delivering quality education, research and innovation by ensuring responsible stewardship of personal and institutional data.

1.3 The University's Core Functions

Universal Technology and Management University (UTAMU) operates under three interdependent core functions: (i) Teaching and Learning; (ii) Research and Innovation; and (iii) Community Engagement and Outreach.

The effective discharge of these functions requires the responsible collection, processing, storage, sharing, and protection of personal and institutional data. This Policy therefore supports the University's triumvirate mandate by ensuring that data governance safeguards academic integrity, research ethics, operational transparency, and public trust.

In doing so, this Policy safeguards the data ecosystems that enable teaching excellence, research credibility, and community accountability.

2.0 THE POLICY

2.1 Authority

This Policy shall be read together with the UTAMU Statute on Governance and Management, UTAMU Risk Management Framework, UTAMU Information Governance Statute and Control Code, Information Security Policy, Records Management Policy, Research Ethics Policy, AI Use Policy, Human Resource Manual, and the Data Protection and Privacy Act, 2019 (Cap 97).

2.2. Purpose

This policy protects the fundamental rights and freedoms of data subjects including students, applicants, staff, alumni, research participants and institutional partners, and establishes institutional readiness mechanisms for lawful, secure and accountable data processing.

2.3. Scope

This Policy applies to all prospective, current and former students; alumni; staff; research participants; contractors; vendors; digital systems; and physical records managed by UTAMU.

2.4 Policy Principles

UTAMU shall process, store, and manage personal data in accordance with the following foundational principles, which guide institutional conduct and control design:

1. **Lawfulness, Fairness, and Transparency**: Personal data shall be processed on a lawful basis, in a manner that is fair to data subjects, and with transparent communication regarding purpose, rights, and safeguards.
2. **Purpose Specification and Limitation**: Personal data shall be collected for specified, explicit, and legitimate institutional purposes aligned to the University's

core functions, and shall not be processed in a manner incompatible with those purposes.

3. **Data Minimization and Storage Limitation**: Only data necessary for the defined purpose shall be collected and retained. Personal data shall not be stored longer than required by legal, academic, regulatory, or operational necessity.
4. **Integrity, Confidentiality, and Security by Design**: Appropriate technical and organisational measures, including encryption and access controls, shall be implemented from data capture through lawful archival or disposal.
5. **Privacy by Design and Default**: Privacy safeguards shall be embedded proactively within system architecture, academic platforms, research processes, and administrative workflows, rather than applied retroactively.
6. **Accountability and Evidence of Compliance**: The University shall maintain documented evidence demonstrating compliance with this Policy, the UTAMU Risk Management Framework, and applicable law. Control effectiveness shall be subject to periodic review and independent assurance.

These principles shall inform control design, system procurement, vendor selection, research protocols, and institutional decision-making involving personal data.

2.5. Data Subject Rights

Data subjects have the right to be informed of processing purposes and legal basis, and shall have access to their personal data, request rectification, or erasure where lawful, exercise data portability, lodge complaints with supervisory authorities.

2.6 Governance Architecture

This Policy operates within the governance hierarchy established under the UTAMU Statute on Governance and Management and shall be implemented in alignment with the UTAMU Risk Management Framework and the UTAMU Information Governance Statute and Control Code. Governance responsibilities are structured to distinguish constitutional authority, executive accountability, operational execution, and independent assurance.

2.7 Constitutional Governance

- **University Council – Formulation and Oversight Authority**: The University Council formulates and aproves this Policy, exercises oversight over its implementation, and reviews annual data governance performance reports prior to escalation to the Board of Directors.
- **Board of Directors – Final Approval Authority**: The Board of Directors shall receive escalated reports relating to High or Critical risk exposures in accordance with the UTAMU Risk Management Framework.

2.7.1 Executive Accountability

Vice Chancellor – Executive Accountability: The Vice Chancellor bears executive responsibility for ensuring institutional compliance with this Policy and for maintaining appropriate governance controls across the University.

2.7.3 Operational Governance

- **head ICT Services – Operational Lead**: The Head ICT Services is responsible for technical implementation, system safeguards, breach coordination, and control effectiveness monitoring.
- **Offices Data Owners – Functional Responsibility**: Admissions, Registry, Finance, Graduate School, Human Resources, and other relevant offices are responsible for lawful data processing within their functional domains and for ensuring compliance with this Policy in day-to-day operations.

2.7.4 Independent Assurance

Office of Internal Audit and Risk – Compliance Verification: The Office of Internal Audit and Risk provides independent assurance on control design, effectiveness, and adherence to statutory obligations and institutional policies.

2.7.5 Reporting and Escalation

An Annual Data Governance Report shall be submitted to the University Council for review and recommendation to the Board of Directors.

Risk-rated High or Critical data governance incidents shall be escalated in accordance with thresholds defined under the UTAMU Risk Management Framework, including mandatory Board notification where required.

2.8. Student Lifecycle Governance

Data protection obligations apply across application, admission, registration, teaching and learning systems, assessment, graduation, alumni engagement, archival retention and lawful disposal.

2.9. Research and AI Governance

All research data must comply with institutional ethics approval, informed consent, anonymisation safeguards and secure storage requirements. AI-assisted systems must comply with institutional data governance controls and cross-border data safeguards.

2.10. Governance and Compliance Architecture

a) Formulation, Approval and Oversight: University Council.
b) Overall Oversight Authority: Board of Directors.
c) Executive Accountability: Vice Chancellor (VC).
d) Operational Lead: Director ICT.
e) Offices of Data Owners: Admissions, Registry, Finance, Graduate School and HR and other relevant offices.
f) Compliance Verification: Office of Internal Audit and Risk. Annual Data Governance Report shall be submitted to the University Council for review and recommendation to the Board of Directors.

2.11. Data Breach Escalation Protocol

All suspected breaches shall be reported immediately to the Head ICT Srvices, escalated to the Vice Chancellor, reported to the University Council, and escalated in accordance with the risk classification thresholds defined under the UTAMU Risk Management Framework, including mandatory Board notification for High or Critical risk events. Incident reporting shall comply with statutory timelines.

2.12. Non-Compliance

Violation of this policy may result in disciplinary action up to and including termination of employment or student expulsion, subject to due process.

2.13. Related Policies and Legal References

This Policy shall be read together with the UTAMU Information Governance Statute and Control Code, UTAMU Statute on Governance and Management, UTAMU Risk Management Framework, Information Security Policy, Records Management Policy, Research Ethics Policy, AI Use Policy, Human Resource Manual, and the Data Protection and Privacy Act, 2019 (Cap 97).

2.14. Responsibility Assignment (RACI) Chart

To ensure clarity of governance roles and accountability across the University, this Policy adopts the RACI framework as a structured responsibility allocation mechanism.

RACI is a widely recognised governance tool used to define and distinguish roles in institutional decision-making and control processes. It prevents ambiguity by clearly identifying who performs an activity, who holds ultimate accountability, who must be consulted, and who must be kept informed.

Under this framework:

- **Responsible (R):** The individual or office that performs the work or executes the task.
- **Accountable (A):** The individual or body ultimately answerable for the outcome and for ensuring the task is completed appropriately. Only one entity should be Accountable for each activity.
- **Consulted (C):** Individuals or offices whose input is required before a decision or action is taken.
- **Informed (I):** Individuals or offices that must be kept apprised of decisions or actions taken.

The RACI framework does not dilute statutory or constitutional authority. Rather, it operationalises institutional governance by clarifying execution pathways within the hierarchy established by the Board of Directors and the University Council.

The matrix below reflects UTAMU's governance structure, ensuring that formulation authority, approval authority, executive accountability, operational responsibility, and audit oversight are clearly distinguished.

RACI Matrix

Governance Activity	Council	Board	VC	Head ICT	Director Internal Audit and Risk
Policy Formulation	A	I	C	C	C
Data Breach Oversight	C	A (High/Critical)	R	R	C
Annual Compliance Reporting	R	A	C	C	R
High/Critical Risk Escalation	C	A	R	R	C

3.0 FINAL PROVISIONS

3.1 Interpretation

This Policy shall be interpreted in alignment with the UTAMU Statute on Governance and Management, the UTAMU Risk Management Framework, the UTAMU Information Governance Statute and Control Code, and the Data Protection and Privacy Act, 2019 (Cap 97).

3.2 Supremacy

In the event of conflict between this Policy and any subordinate procedure, guideline, or operational instruction, this Policy shall prevail to the extent of the inconsistency.

3.3 Review and Continuous Improvement

This Policy shall be reviewed at least once every five (5) years, or earlier where required by regulatory change, risk assessment findings, audit recommendations, or directive of the Board of Directors.

3.4 Amendment Authority

Any amendment to this Policy shall follow the same formulation and approval pathway as the original instrument, namely formulation and recommendation by the University Council and approval by the Board of Directors.

3.5 Effective Date

This Policy shall take effect on the date of approval by the University Council unless otherwise specified.

Signed on this.....27th.....day of .....March..... 2026

By:

.....

Chairperson, University Council

.....

Vice Chancellor