Redeemer's University, Ede

Data Protection Policy

Effective Date: 1st September, 2025
Review Cycle: Every three years or as required by law

1. Introduction

Redeemer's University is committed to the lawful, secure, and ethical handling of all personal and institutional data in its care. As a faith-based institution dedicated to truth, integrity, and stewardship, the university recognizes the importance of respecting the privacy and dignity of all individuals whose data it collects, stores, processes, or shares.

This policy outlines how the University ensures compliance with the Nigeria Data Protection Regulation (NDPR) and other applicable data protection laws.

2. Objectives of the Policy

This policy aims to:

- Protect the privacy rights of students, staff, alumni, research participants, and third parties.
- Ensure that all personal data is processed lawfully, fairly, and transparently.
- Establish responsibilities for data governance, compliance, and breach management.
- Safeguard institutional integrity and public trust in the University's information systems.

3. Scope

This policy applies to:

- All staff, students, faculty, consultants, vendors, and partners who process or manage personal data on behalf of Redeemer's University.
- All data types, whether stored digitally or physically, including:
    - Student records
    - Employee files
    - Medical data
    - Financial information
    - Research data
    - Biometric or CCTV footage

4. Key Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable person (e.g., name, ID, email, biometrics).
Data Subject	The individual whose personal data is being collected or processed.
Data Controller	The University, which determines how and why personal data is processed.
Data Processor	Any entity processing data on behalf of the University.
Processing	Any operation performed on data (collection, storage, use, sharing, deletion, *etc*.).

5. Data Protection Principles

Redeemer's University adheres to the following core principles:

1. **Lawfulness, Fairness, and Transparency**
    - Data shall be processed legally and in a way that is fair and understandable to the data subject.
2. **Purpose Limitation**
    - Data shall be collected for specified, explicit purposes and not used for unrelated purposes.
3. **Data Minimization**
    - Only the minimum necessary data shall be collected and processed.
4. **Accuracy**
    - Data must be accurate and kept up to date.
5. **Storage Limitation**
    - Data shall not be retained longer than necessary for the intended purpose.
6. **Integrity and Confidentiality**
    - Data must be securely protected against unauthorized access, loss, or damage.
7. **Accountability**
    - The University must demonstrate compliance with all data protection requirements.

6. Lawful Basis for Processing

The University may process personal data under the following lawful bases:

- Consent of the data subject
- Performance of a contract (e.g., employment, student admission)
- Legal obligation
- Vital interest (e.g., health emergencies)
- Public interest or legitimate university function

7. Data Subject Rights

Data subjects have the right to:

- Be informed of how their data is used
- Access their personal data
- Rectify inaccurate data
- Erase their data under certain conditions
- Restrict or object to data processing
- Data portability (where applicable)
- Lodge a complaint with the University

8. Data Collection and Processing Guidelines

All departments and units must:

- Collect data using transparent forms with consent notices.
- Avoid requesting excessive or irrelevant personal data.
- Ensure that third-party processors (e.g., cloud services) are under data protection agreements.
- Store physical files in locked cabinets and electronic files on secure servers with access control.
- Avoid sharing sensitive data via unsecured email or devices.

9. Special Categories of Data

The following types of data require enhanced protection:

- Health and medical records
- Biometric data (e.g., fingerprints, facial scans)
- Student disciplinary records

- Financial and payment information

10. Data Breach and Incident Response

In the event of a suspected data breach:

1. Report immediately to the Data Protection Officer (DPO).
2. The DPO shall assess the breach and notify the Nigeria Data Protection Commission (NDPC) within 72 hours **if required**.
3. Affected individuals shall be informed if there is a high risk to their rights or freedoms.
4. A post-incident review will be conducted, and corrective action taken.

11. Data Retention and Disposal

- Data should only be kept as long as necessary, based on the **University's Data Retention Schedule**.
- Outdated digital files must be securely deleted.
- Physical records must be shredded or incinerated in line with university policy.

12. Roles and Responsibilities

Office/Unit	Responsibility
Vice-Chancellor	Provides overall leadership and commitment to compliance.
University Senate	Approves this policy and reviews updates.
Data Protection Officer (DPO)	Oversees implementation, compliance, training, and reporting.
ICT Directorate	Ensures cybersecurity, infrastructure security, and access control.
All Departments	Ensure compliance in data collection and use.
Staff and Students	Handle personal data responsibly and report breaches.

13. Training and Awareness

- All staff and students shall undergo **annual training** on data protection principles.
- Data privacy statements and consent forms shall be included in all registration, admission, and employment portals.

- Periodic awareness campaigns will be run via university communication platforms.

14. Third-Party Data Processors

Any third-party vendor or service provider handling personal data must:

- Sign a **Data Processing Agreement (DPA)** with the University.
- Meet the same data protection and security standards required by this policy.
- Be vetted by the ICT and Legal Units.

15. Compliance and Penalties

Failure to comply with this policy may result in:

- Internal disciplinary action (including sanctions or dismissal)
- External penalties from NDPC
- Suspension or cancellation of data-sharing contracts

16. Review and Updates

This policy shall be:

- Reviewed every **two years** or sooner as required by law or regulatory changes.
- Updated in consultation with the DPO, ICT, Legal Unit, and relevant departments.

17. Contact

For any concerns or questions regarding data protection, contact:

Mr. Samuel A Adenle
Data Protection Officer (DPO)
Email: dpo@run.edu.ng
Office: Zenith ICT building, Redeemer's University, Ede.
Phone: +2347063313424

Appendices

- **Appendix A:** Data Retention Schedule
- **Appendix B:** Data Breach Reporting Template
- **Appendix C:** Staff & Student Data Consent Forms
- **Appendix D:** List of Approved Third-Party Data Processors