RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

# Protection of Personal Information Policy

| | |
|---|---|
| **Policy Volume** | General Institutional Policies/Protocols/Guidelines |
| **Policy Chapter** | General Institutional Policies/Protocols/Guidelines |
| **Responsible Committee/Unit/Division/Faculty** | IPC |
| **Responsible Chairperson/Director/Manager** | Registrar |
| **Dates of First and Subsequent Council Approvals** | September 2021 |
| **Policy Approval Pathways (e.g. committee, Senex, Senate, Council)** | IPC, Senex, Senate, Council |
| **Revision History: Approved Reviews** | N/A |
| **Review Cycle (e.g. every 2/5/7 years etc)** | 5 years |
| **Next Review Date** | 2026 |

## 1. POLICY PARTICULARS

| | |
|---|---|
| **1.1. Policy Title** | Protection of Personal Information |
| **1.2. Policy Statement**<br>(State in a single paragraph the policy mandate and how this relates to the University Mission and Vision) | This Policy guides protection of, dissemination of and destruction of personal information in all formats; electronic, paper, localised copies of information and information stored on servers within the University framework |
| **1.3. Reason for Policy**<br>(What this policy aims to achieve) | The Protection of Personal Information Act gazettes the manner in which Institutions must comply in order to give effect to the constitutional right to privacy and to ensure that penalties<br>are avoided. The University is bound to the Act and the Policy is an internal document intended to guide behaviour at all levels within the University |
| **1.4. Policy Objective/s**<br>(What are the measurable objectives of this policy) | The Policy objective is to regulate behaviour in order to ensure that the University complies with the Protection of Personal Information Act, whilst at the same time allowing access to information to any party who has the<br>right thereto in terms of the Promotion of Access to Information Act. |
| **1.5. People affected by this Policy**<br>(e.g. All units of the University) | All University employees |
| **1.5. Who should read this Policy?**<br>(People who need to heed this policy to fulfil their duties) | Employees within HR Division, Registrar's Division, Information and Technology Services Division, Finance Division, Infrastructure and Operations, Library Services Employees within academic departments and Research entities who have access to personal information<br>Researchers who require information from the University databases to conduct research<br>All employees who have access to personal information housed in a database or on paper |
| **1.6. Implementers of this Policy**<br>(Who will manage the implementation of this policy) | All persons in an information or deputy information officer capacity. |
| **1.7 Website address/link for this Policy** | |

## 2. RELATED DOCUMENTS FORMS AND TOOLS

(University Policies, Protocols and Documents (such as rules/policies/protocols/guidelines related to this policy)

| |
|---|
| **Relevant Legislation** (Legislation/Regulatory requirements/Organisational Reports – name these) |
| Constitution of the Republic of South Africa,<br>1996 Protection of Personal Information Act<br>4 of 2013 Promotion of Access to<br>Information Act 2 of 2000 |
| **Related Policies** |
| Emergency Access to Electronic<br>Information Email Policy<br>Centralised Database Policy |
| **Related Protocols** |
| |
| **Forms and Tools** (documents to be completed in support of this policy implementation) |
| E.g. Policy template for the policy itself. Documents pertaining to procedures for implementation, as well as monitoring and evaluation of the policy. |

## 3. POLICY DEFINITIONS

(Technical or Conceptual terms used in the policy)

| No | TERM | DEFINITION |
|---|---|---|
| **3.1** | **Data** | **Isolated Facts** |
| **3.2** | **Information** | **Organised or summarised data** |
| **3.3** | **Database** | **A collection of interrelated data items, usually electronic** |
| **3.4** | **DBMS** | **Database Management System – system software that facilitates the management of a database** |
| **3.5** | **Dataset** | **The result of a query on the database that provides a subset of the data housed in the database** |
| **3.6** | **Platform** | **The computer technology (hardware and software) or paper used to store and access the information** |
| **3.7** | **Summarised Data** | **Data that has been collated into numeric values, removing any link to an individual's identity** |
| **3.8** | **Detailed Data** | **Data that is related and identifies individuals** |
| **3.9** | **Anonymous Data** | **Data that has been de-linked from individuals by removing information such as employee numbers, student numbers, identity numbers and personal contact information or identification** |

## 4. PRINCIPLES GOVERNING THIS POLICY

| **OVERVIEW** |
|---|
| Rhodes University strives to carry out the following, as far as is reasonably practicable: |
| 4.1. Grant access to information only where a party has the right to such information or when necessary in order to process administration and conduct relevant research |
| 4.2. Protect information by following the implementation procedures laid out in this policy |
| 4.3. |
| **4.4.** |
| **4.5.** |
| **4.6.** |

## 5. DIRECTIVES FOR IMPLEMENTING THIS POLICY

(Actions and processes by which the objectives of the policy will be achieved.)

**5.1.** In order to ensure compliance, departments and faculties with access to information must follow correct process when managing information.

1) Access to student, alumni and staff information must be regulated and properly managed. Detailed information must be masked and delivered only where there is a right to such information, and then only if the information is important and useful.

2) Administrative staff, Deans and Heads of Departments, responsible for requesting access to information must consider appropriate levels of access and not grant blanket access to individuals who do not require the information in order to carry out work responsibilities. .

3) Student information pages accessible to departments will not display identity numbers, race and gender nor financial information. Financial information will only be visible to sections that require it in order to assist students.

4) Those requesting information are required to use centralised information services and systems in order to protect access to information. In cases where information is extracted for analysis, the information should be anonymous or removed from the device where it is stored when the analysis is complete.

5) Data sets should be appropriately scaled in size to ensure that n=1 does not begin to identify individuals within the dataset.

6) Email lists or phone numbers will not be provided to external requestors. The University may send an email or SMS on behalf of an approved requestor

**Data Requests from Centralised Data**

1) All emailed requests must be made by emailing the relevant deputy information officers.

2) Telephonic requests are suggested if discussion with MIS is required before the request can be formalised.

3) Data requiring personal details rather than summarised or anonymous data may be referred to the Registrar or Director of HR for approval. A central repository of requests and outcome will be maintained by the University.

4) Information submitted to DHET and any other legislative bodies will continue as required.

5) Redacted information and datasets can be approved by the I&TS MIS section acting as an agent for the Registrar or HR, provided that the individual making the request would usually have access to this information. Any other request must be approved by the Registrar or Director HR.

6) Requests to email research participation to employees must be approved by HR. HR must also indicate to I&TS to whom the request will be emailed and the content of the email.

7) Individual's personal information may not be extracted and used to contact individuals if the individual has indicated they do not wish to receive information of the nature of the communique. Registered students and current staff may not opt out of University messages.

8) All requests for data, including requests for Alumni information must be recorded in the central repository.

9) Individuals receiving the information must password protect the information in a directory that is accessed via authentication or by a password.

10) Departments and individuals may not extract information into spreadsheets that are not protected.

**Life of Information**

1) Financial information pertaining to individuals will be kept according to fiduciary practices (currently 10 years). Information relating "bad debts" will be cleared once the payment is made, unless the University policy dictates that the student may not return to the University, in which case a secondary indicator will be held to prohibit re-registration.

2) Information relating to student academic records will be kept indefinitely as this information is necessary for producing transcripts and academic course records.

3) Information relating to student biographic details will be kept indefinitely for historic research and analytic comparisons to be processed.

4) Information related to year of registration ie. Banking details, addresses and phone numbers will be cleared 5 years after final year of registration.

5) Alumni information will be kept indefinitely but alumni may opt out and contact information will then be removed from the database.

6) Detailed employee information will be kept indefinitely including last position held, employee number, name and ID number. Keeping the same identity is an important part of determining length of service as well as linking historical research outputs, student supervision and email/internet identity.

## 6. ROLES AND RESPONSIBILITIES

(Roles and responsibilities of Key personal/Divisions/Faculties/Departments)

| ROLE | RESPONSIBILITY |
|---|---|
| **REGISTRAR** | Approval of student data provisioning to requestor after ethics approval and interrogation of the requirement. |
| **Director HR** | Approval of employee data provisioning to requestor after ethics approval and interrogation of the requirement. Training of all employees regarding the POPI and compliance |
| **I&TS** | Distribution and record keeping of electronic information held centrally |
| **All staff** | Protection of any lists and spreadsheets in authentication required directories or with a password protection. |

## 7. CONTACTS

| Area of Concern | Division/Faculty/Department | Telephone | Email |
|---|---|---|---|
| Registrar | Registar's Division | | |
| Director HR | Human Resources | | |
| Director I&TS | Information and Technology Services | | |
| | | | |

## 8. POLICY REVIEW PROCEDURE

(Actions and processes by which the policy will be reviewed)

| |
|---|
| IPC will review the Policy every 3 years unless legislation requires an immediate overhaul within the cycle |
| **Communication of the review process** |

## 9. POLICY CONTEXT: RELEVANT DOCUMENTS CITED/CONSULTED/ADOPTED

| | |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |

## LIST OF APPENDICES