


UWC			
 <p>UNIVERSITY of the WESTERN CAPE</p>	<p><b>PROTECTION OF PERSONAL INFORMATION POLICY</b></p>	Council Approval Reference Number First Approval Amendments	C2021/03 (29 June 2021)
		Implementation Date	July 2021
		Revision / Amendment	<b>C2022.04</b> - review and update to clause 5 (roles and responsibilities of IO; DIO and Legal services)
		Revision / Amendment Date	1 December 2022 (C2022.04)
		Provisos	N/A
		Policy Owner	Registrar
		Executive Management Portfolio	Registrar
		Contributors	EMC, Senate, IF, CRG Council Amendments: EMC, PIRG (previously CRG), Council
		Circulated by:	Registrar
		Circulated to:	Campus Community

## PROTECTION OF PERSONAL INFORMATION POLICY

## PROTECTION OF PERSONAL INFORMATION POLICY

<b>Policy name</b>	University of the Western Cape Protection of Personal Information Policy
<b>Executive responsible</b>	Registrar
<b>Policy drivers</b>	Senior Management, Directors and Heads of Departments
<b>Governance</b>	<u>Consultation</u> Institutional Forum: 18 February 2021 Senate: 23 February 2021 Council: 25 March 2021 <u>Final Approval</u> <b>Council: 29 June 2021</b>
<b>Policy life-cycle</b>	Every three years
<b>Relevant Legislation</b>	Protection of Personal Information Act 4 of 2013 Promotion of Access to Information Act 2 of 2000
<b>Institutional policies</b>	USAf POPIA Industry Code of Conduct: Public Universities ICT Information Security Policy
<b>International Standards and Guidelines</b>	ISO 27001; ISO 31000

# TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>3</b>
<b>2. PURPOSE STATEMENT</b>	<b>4</b>
<b>3. PRINCIPLES</b>	<b>4</b>
3.1. Information security management	4
3.2. Privacy protection	4
3.3. Records management	6
<b>4. PERFORM PERSONAL INFORMATION IMPACT ASSESSMENTS</b>	<b>8</b>
<b>5. ROLES AND RESPONSIBILITIES</b>	<b>9</b>
<b>6. DEFINITIONS</b>	<b>12</b>
<b>7. POLICY FORMULATION PROCESS</b>	<b>14</b>

## **1. Introduction**

The University of the Western Cape (the University) values the trust our students, employees, service providers, suppliers, partner institutions, funders, research participants, members of the public and other data subjects place in us when they share personal information with us. Without this personal information, we would not be able to function effectively, so it is crucial that we protect it in accordance with the principles set out in the Protection of Personal Information Act (POPIA).

This policy must be read together with the:

- Information Security Policy
- Document, Records and Archives Management Policy and Retention Schedule

## **2. Purpose statement**

The purpose of this policy is to help guide the University's actions so that we keep personal information safe, protect our reputation, and comply with all relevant data protection regulations, including the Protection of Personal Information Act (POPIA).

This policy applies to:

- All personal information used, transformed or produced by the University;
- anybody involved in the processing of personal information; and
- all employees, students, researchers, service providers, contractors, and other individuals who have access to personal information.

## **3. Principles**

It is the University's policy to follow the principles of:

- Information security management;
- Privacy protection; and
- Records management.

### **3.1. Information security management**

The University secures information against

- breaches of confidentiality;
- failures of integrity; and
- interruptions to the availability of information.

The University follows the policy statements set out in its Information Security Policy.

The University manages risks to the security of personal information by:

- identifying and reviewing all the internal and external information security risks that we can reasonably foresee;
- ensuring that we have adequate security safeguards in place at each stage of the lifecycle of our systems and processes;
- maintaining appropriate safeguards against the risks we identify;
- regularly verifying that we implement the safeguards effectively; and
- ensuring that we continually update the safeguards in response to new risks or deficiencies in the safeguards.

### **3.2. Privacy protection**

To ensure compliance with POPIA and that the University respect the right to privacy, we follow the principles of privacy protection when we process personal information:

Principle	What the University does
Classify personal information	We identify and classify the personal information we use.
Document personal information processing activities	We document all processing activities to ensure that we can respond to requests from the Information Regulator and requests for information by data subjects or third parties.
Specify the purpose of processing personal information	We specify and document the purposes for which we process personal information.
Provide a legal basis for processing activities	<p>We ensure that all processing activities have a legal basis. We only process personal information if it:</p> <ul style="list-style-type: none"> <li>• is necessary to conclude to perform in terms of a contract;</li> <li>• is required to comply with legislation;</li> <li>• is necessary for the proper performance of our function as a public university;</li> <li>• protects the legitimate interest of a data subject; and</li> <li>• is necessary to protect our or a third party's legitimate interests.</li> </ul> <p>If none of these legal bases apply, we must ask the data subject's consent before we process their personal information. However, this consent must be a specific, informed and voluntary expression of will.</p> <p>We document the specific legal basis for processing personal information for each activity.</p>
Keep processing to a minimum	<p>We ensure that:</p> <ul style="list-style-type: none"> <li>• we only process personal information that is adequate, relevant and not excessive, considering the purpose of the activity; and</li> <li>• we de-identify personal information before we start the activity where possible.</li> </ul>

Obtain personal information from lawful sources	We obtain personal information from lawful and dependable sources only. We prefer to collect personal information from the data subject directly.
Process transparently	We disclose all processing activities to data subjects in our privacy notices.
Ensure personal information quality	We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.
Limit sharing	We only share personal information if it is legal to do so and ethically justifiable. We enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information. We keep a record of when we share personal information, whom we shared it with, and the method we used to transmit personal information.
Respect data subjects' rights	We respect the rights of data subjects to: <ul style="list-style-type: none"> <li>• access their records;</li> <li>• know whom their information was shared with;</li> <li>• correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information;</li> <li>• withdraw consent; and</li> <li>• object to the processing of their information when it is not necessary for the conclusion or performance of a contract or to comply with an obligation imposed by law.</li> </ul>

### 3.3. Records management

The University manages the records we create, receive, and maintain to ensure that our recordkeeping:

- is transparent, consistent, and accountable;
- meets legal, regulatory, fiscal, and operational requirements; and
- supports the efficient conduct of the University.

This policy must be read with the Document, Records and Archives Management Policy and the Records Retention Schedule.

The University follows these principles of records management:

Principle	What the University does
Create, approve and maintain a records retention schedule.	<p>Our records retention schedule contains:</p> <ul style="list-style-type: none"> <li>• a list of categories of records that must be maintained for legal, regulatory, or business requirements;</li> <li>• a default retention rule for each category of records;</li> <li>• any exemptions to the default rule;</li> <li>• the reason for retention;</li> <li>• the period for which the category of records must be retained; and</li> <li>• the event that triggers the start of the period.</li> </ul>
Apply effective version control practices	<p>We ensure that:</p> <ul style="list-style-type: none"> <li>• version control practices are implemented for all records to ensure that the correct version of the record is retained; and</li> <li>• a reliable record of all activities of users is maintained and monitored to detect unauthorised or irregular handling of records.</li> </ul>
Minimise duplication	<p>We ensure that we minimise the duplication of records by identifying and controlling master records.</p>
Records are adequately preserved	<p>We have a process in place to ensure that records are adequately preserved when employees, service providers, contractors, or other individuals who have access to our information leave.</p>
Records are securely destroyed	<p>When a record no longer needs to be retained, the Information Officer must confirm whether the record must be:</p> <ul style="list-style-type: none"> <li>• securely destroyed; or</li> <li>• in exceptional circumstances relating to that specific record, retained for another specified period.</li> </ul>

	We keep a record of what records were destroyed, the date on which they were destroyed, and the method used.
Train employees on their responsibilities	We train all employees and temporary employees on the recordkeeping requirements that apply to the information to which they have access.

#### **4. Perform personal information impact assessments**

Senior Management and Directors and Heads of Departments with the support of the Deputy Information Officers, must ensure that a personal information impact assessment (PIIA) is performed before the University processes the personal information of data subjects. The purpose of a PIIA is to assess, analyse and evaluate risks and compliance with the principles set out in this policy.

A PIIA must be performed before the University:

- continues to process personal information as part of a processing activity which has not undergone a PIIA before;
- changes an existing processing activity materially;
- processes personal information for a new purpose;
- launches new services;
- expands into other countries;
- uses new systems/software in a processing activity; or
- shares personal information with third parties.

During a PIIA:

- the processing activity will be documented;
- the processing activity and any related documents will be assessed against the principles set out in this policy;
- risks and areas of non-compliance with the principles will be identified by the University's Deputy Information Officers;
- the University's Deputy Information Officers will make recommendations on how the risks can be addressed;
- the relevant members of senior management, directors and heads of department will decide whether the recommendations must be implemented or not; and
- an implementation and monitoring plan will be agreed between senior management, directors and heads of department and the Deputy Information Officers.

To initiate a PIIA contact any of the University's Deputy Information Officers.



## 5. Roles and Responsibilities

Role	Responsibilities
Information officer: Rector and Vice-Chancellor	<ul style="list-style-type: none"> <li>• Encourages compliance with the conditions for the lawful processing of personal information.</li> <li>• Deals with requests submitted pursuant to POPIA.</li> <li>• Work with the Regulator in relation to investigations conducted in terms of Chapter 6 of POPIA.</li> <li>• Ensures compliance with the provisions of the POPIA.</li> <li>• Ensures that:               <ul style="list-style-type: none"> <li>i) A compliance framework is developed, implemented, monitored and maintained;</li> <li>ii) A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;</li> <li>iii) A manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, Act No. 2 of 2000 (PAIA);</li> <li>iv) internal measures are developed together with adequate systems to process requests for information or access thereto; and</li> <li>v) internal awareness sessions are conducted regarding the provisions of POPIA, POPIA regulations, codes of conduct, or information obtained from the Regulator.</li> </ul> </li> <li>• Develops, implements, monitors and maintains this policy.</li> </ul>

	<ul style="list-style-type: none"> <li>• Ensures that POPIA compliance receives support from senior management, directors and heads of department throughout the University and that senior management, directors and heads of department discharges their responsibilities.</li> <li>• Creates an environment conducive to the successful implementation of this policy and the management of risks and non-compliance.</li> <li>• Appoints Deputy Information Officers.</li> </ul>
<p>Chief Information Security Officer: Deputy Director: ICT Governance Risk and Compliance</p>	<ul style="list-style-type: none"> <li>• Oversees information security management for all personal information.</li> <li>• Develops procedures and standards to support information security management.</li> <li>• Recommend appropriate technology investments to support the implementation of this policy.</li> <li>• Provides advice to senior management, directors and heads of department on the identification and management of information security risks.</li> <li>• Monitors whether information security risk assessments are performed by senior management and directors and heads of department when required.</li> <li>• Reports to the Information Officer.</li> </ul>
<p>Deputy information officers (Privacy and Records Management): Registrar (student applicants, registered students, international students and alumni]</p>	<ul style="list-style-type: none"> <li>• Oversees compliance with privacy and records management principles in their area of the University.</li> <li>• Develops procedures and standards to support data privacy and records management.</li> <li>• Ensures that investments in infrastructure, process development and automation and training are made to enable compliance with privacy and records management obligations.</li> </ul>

<p>Director: Legal Services (Independent contractors, suppliers and service providers, donors, other organisations with whom the university has a relationship).</p>	<ul style="list-style-type: none"> <li>• Provides advice to senior management, directors and heads of department on the identification and management of privacy risks.</li> <li>• Monitors whether personal information impact assessments are performed by senior management, directors and heads of department when required.</li> <li>• Reports to the Information Officer.</li> <li>• Any power or duty conferred or imposed on the information officer as set out above.</li> </ul>
<p>Executive Director: Human Resources (employment candidates, employees, visiting academics, former employees, student employees)</p>	
<p>Legal Services</p>	<ul style="list-style-type: none"> <li>• Provides advice on the interpretation of legislation and incidents, including POPIA.</li> <li>• Provides advice to employees in respect of their contractual obligations and their responsibility to manage contract risk.</li> </ul>
<p>Internal and external audit</p>	<ul style="list-style-type: none"> <li>• Provides independent assurance that University's risk management, governance and internal control processes are operating effectively, including the implementation of this policy.</li> <li>• Reports to Council.</li> </ul>
<p>Senior Management and Directors/Heads of Department of Departments, Units, Centres, Schools and Institutes</p>	<ul style="list-style-type: none"> <li>• Ensures that this policy is implemented in their area and that the management of personal information becomes part of the accepted way of working.</li> <li>• Ensures that personal information impact assessments are performed when required.</li> </ul>
<p>All employees, students, researchers, service providers, contractors, and other individuals who have access to personal information (users).</p>	<p>All individuals with access to personal information must:</p> <ul style="list-style-type: none"> <li>• comply with the University's code of conduct, end-user manual or other</li> </ul>

	<p>rules relating to the handling of personal information.</p> <ul style="list-style-type: none"> <li>• report security incidents and non-compliance with this policy to a Deputy Information Officer as soon as they become aware of or suspect that an incident has taken place or is about to take place.</li> </ul>
--	---

## 6. Definitions

Data Subject	<p>The person or organisation to whom the personal information relates. This includes:</p> <ul style="list-style-type: none"> <li>• prospective students, students, and alumni;</li> <li>• staff members, job applicants, and functionaries;</li> <li>• service providers, contractors, and suppliers;</li> <li>• partner institutions, and funders;</li> <li>• research participants;</li> <li>• members of the public and visitors.</li> </ul>
Information	<p>All data, records, and knowledge that forms part of the intellectual capital the University uses, transforms, or produces. It includes public, private, confidential, and personal information.</p>
Information asset	<p>An information asset is a body of information that is organised and managed as a unit. Examples include:</p> <ul style="list-style-type: none"> <li>• a database, whether it is an Excel spreadsheet or in an information management system;</li> <li>• a folder in which we keep all information relating to a particular topic in a centrally accessible location (e.g. SharePoint or Google Drive); and</li> </ul>

	<ul style="list-style-type: none"> <li>physical records stored in a filing cabinet.</li> </ul>
Personal information	<p>Information relating to an identifiable individual or an existing organisation (data subjects), including:</p> <ul style="list-style-type: none"> <li>identifiers such as a name, identity number, staff number, customer number, company registration number, tax number, photos, and videos</li> <li>demographic information such as race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, physical or mental health or wellbeing, disability, religion, conscience, belief, culture, language, and birth</li> <li>background information such as education, financial, employment, medical, criminal, or credit history</li> <li>contact details such as a physical and postal address, email address, telephone number, online identifier, or location information</li> <li>biometric information such as blood type, fingerprints, DNA analysis, facial recognition, retinal scanning and voice recognition</li> <li>someone's opinions, views and preferences</li> <li>private or confidential correspondence</li> <li>views and opinions about a person, such as interview notes and trade references</li> <li>the criminal behaviour of a data subject to the extent that it relates to the alleged commission of an offence</li> <li>any proceedings in respect of any offence allegedly committed by a data subject</li> </ul>
POPIA	The Protection of Personal Information Act 4 of 2013, its regulations and any accredited industry code.

Processing	Any operation or activity or any set of functions concerning personal information, including: <ul style="list-style-type: none"> <li>collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using;</li> <li>disseminating through transmission, distributing, or making available in any other form; or</li> <li>merging, linking, restricting, degrading, erasing or destroying personal information.</li> </ul>
Record	Information created, received and maintained by the University as evidence of actions or decisions, to meet legal, regulatory, fiscal, operational and historical requirements.
The University	The University of the Western Cape
Third Party	External organisations or individuals
Users	All employees, students, researchers, service providers, contractors, and other individuals who have access to personal information.

## 7. Policy formulation process

	Contributors	Details	Date
1	The Registrar	Initial draft	11/02/2021
2	Institutional Forum	No comments/suggestions	18/02/2021
3	Senate	No comment/suggestions	23/02/2021
4	Council	Reference to ISO 31 000 to be incorporated.	25/03/2021
5	Council	Final approval	29/06/2022
<b>Amendments</b>			
6	EMC	No comments	8 August 2022

7	Personal Information Reference Group (PIRG), previously CRG	No comments	27 July 2022; 27 September 2022
8	Council	Approved amendments	1 December 2022