

https://dspace.org/

The Wits Protection of Personal Information Act (POPI) Policy

University of the Witwatersrand, Johannesburg

2021
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/49999
University of the Witwatersrand, Johannesburg. (2021). The Wits Protection of Personal Information Act (POPI) Policy. WIReDSpace. https://hdl.handle.net/10539/49999

Downloaded from a DSpace repository. https://dspace.org/



UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

The Wits Protection of Personal Information Act (POPI) Policy

Version No.1

TABLE OF CONTENTS

1.	**Context / Background**	**3**
2.	**Definitions**	**3**
3.	**Purpose**	**4**
4.	**Principles**	**5**
5.	**Roles and Responsibilities**	**5**
6.	**Privacy Notice**	**5**
7.	**Annexures**	**7**
	Annexure A:Processing	**7**
	Annexure B:Categorisation of Personal Information Processed	**14**

Policy Title	Wits POPI Policy
Policy Officer	Carol Crosley
Date Approved	2021
Date Effective From	2021
Last updated	2021

1. Context and Background

This policy covers The University's compliance with and application of the Protection of Personal Information Act, 4 of 2013 ("POPIA"). The University promotes the right to privacy and the POPIA includes the right to protection against unlawful processing of Personal Information, giving effect to the right to privacy as enshrined in section 14 of the Constitution of the Republic of South Africa.
The University is committed to protecting Data Subjects' privacy and recognises the importance of compliance with statutory requirements in the collection, transfer, retention, and distribution of Personal Information (referred to as "processing").

2. Definitions

Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	The person to whom personal information relates, and for purposes of this policy includes, but is not limited to, the University's: governance and/or appointed officer-bearers, prospective students, students, researchers, research participants, post-doctoral fellows, alumni, authors, employment candidates, employees, external members of committees, council members, partner organisations, subsidiaries, donors and funders, visitors, contractors, service providers, agents, members of the public.
De-identify	To delete any information that identifies the Data Subject, can be used or manipulated by a reasonably foreseeable method to identify the Data Subject, or can be linked by a reasonably foreseeable method to other information that identifies the Data Subject.
Information Officer	The Information Officer required in terms of section 55 of the POPIA;
Deputy Information Officer	The Deputy Information Officer required in terms of section 56 of POPIA;
'Information Regulator	The Information Regulator established in terms of section 39 of POPIA.
Operator	A person who processes Personal Information for The University in terms of a contract or mandate, without coming under the direct authority of The University.
Person	A natural person or a juristic person;

Personal Information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person (whether The University employees, directors, customers, suppliers, contractors, shareholders, or contractors' or suppliers' staff), including, but not limited to: a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; b. information relating to the education or the medical, financial, criminal or employment history of the person; c. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d. the biometric information of the person; e. the personal opinions, views or preferences of the person; f. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g. the views or opinions of another individual about the person; and h. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person; i. and includes ''**special personal information**'' referred to in section 26 of the POPIA such as religion, race or ethnic origin, criminal record, trade union membership, health, medical records, or biometric information of a Data Subject.
POPIA	The Protection of Personal Information Act, 4 of 2013.
Processing	Any operation or activity or any set of operations, whether by automatic means, concerning Personal Information, including: a. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; b. dissemination by means of transmission, distribution or making available in any other form; or c. merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information.
Responsible Party	The University as a private body, who alone or in conjunction with others, determines the purpose of and means for processing Personal Information.
Privacy Notice	A privacy notice describes how your personal information is used by The University as a result of a person's engagement with The University.
The University	The University of the Witwatersrand, a tertiary institution established in terms of the applicable legislation of the Republic of South Africa.

3. PURPOSE

This policy promotes the protection of Personal Information and aims to regulate, in harmony with regulatory standards, the processing of Personal Information by The University, as well as promotion of the right to privacy and regulation of the manner in which The University Processes Personal Information, in accordance with the requirements of the POPIA.

4. PRINCIPLES

4.1 This policy applies to all The University operations and activities in South Africa and to the extent legally required in other jurisdictions, and to The University's, including but not limited to, governance and/or appointed officer-bearers, prospective students, students, researchers, research participants, post-doctoral fellows, alumni, authors, employment candidates, employees, external members of committees, council members, partner organisations, subsidiaries, donors and funders, visitors, contractors, service providers, agents, members of the public.

4.2 The University Processes Personal Information of the individuals (natural persons) and corporate entities (juristic persons, such as companies, close corporations and trusts) with whom it works in order to operate and carry out its operations and activities (collectively referred to as "Persons").

4.3 The University regards the lawful and proper processing of Personal Information as crucial to successful service delivery and essential to maintaining confidence between The University and those Persons who deal with it.

5. ROLES AND RESPONSIBILITIES

Information Officer	The University complies with section 55 of the POPIA and an Information Officer has been appointed and registered with the Information Regulator
	The Vice Chancellor of the University has been appointed as The University's Information Officer.
	The Vice Chancellor will be assisted in conducting his duties and responsibilities in terms of section 56 of POPIA by The University's Registrar who has been appointed as Deputy Information Officer.
Deputy Information Officer	Section 17 of PAIA provides for the designation of a Deputy Information Officer of a public body, and section 50(6) of POPIA extends the designation of a Deputy Information Officer for a private body.
	The duties and responsibilities of a Deputy Information Officer should not be in conflict with other duties assigned to him or her; 7.8. A Deputy Information Officer must be accessible to everyone, particularly to a data subject in respect of POPIA or a requester, in terms of PAIA.
	A Deputy Information Officer(s) should have a reasonable understanding of the business operations and processes of a body. An employee(s) with institutional knowledge must be preferred for designation as a Deputy Information Officer(s).

6. PRIVACY NOTICES

The University has a Privacy Notice (https://www.wits.ac.za/popia-and-paia/) which describes how personal information (PI) is used by the University as a result of a person's engagement with the University. This includes how the personal information is collected, how it is used and why it is used.

VERSION HISTORY

Version	Date	Summary	Changed by
1.	September 2021	Wits POPI Policy	Nicoleen Potgieter

Annexure A

1. PROCESSING

The University Processes Personal Information of Persons in accordance with the eight conditions for the lawful processing of Personal Information as contained in the POPIA and these principles guide The University on how Personal Information must be processed. Data Subject consent to process Personal Information is provided voluntarily.

1.1 Eight Conditions for Lawful Processing

- **1.1.1. Accountability**
- **1.1.2. Processing Limitation**
- **1.1.3. Notification of collection and collection for specific purpose**
- **1.1.4. Further Processing Limitation**
- **1.1.5. Information Quality**
- **1.1.6. Openness**
- **1.1.7. Security Safeguards**
- **1.1.8. Data Subject Participation**

1.2 Application of the eight conditions for lawful processing of personal information

CONDITION	INFORMATION	
Condition 1 **Accountability**	Where The University is a Responsible Party for the purposes of Processing Personal Information, it ensures that the eight conditions for the lawful processing of Personal Information as set out in the POPIA, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.	
Condition 2 **Processing Limitation**	**Lawfulness of processing** The University Processes Personal information lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject. In particular, The University's processing of any special personal information of a Data Subject complies with sections 26 through 35 of the POPIA in that it is, amongst other things, only carried out where **(i)** The University has obtained the consent of the Data Subject; **(ii)** it is necessary for the establishment, exercise or defence of a right or obligation in law; or **(iii)** it serves a public interest and the processing is necessary for the purpose concerned.	**Minimality**: The processing activities of The University is regarded as adequate, relevant, and not excessive.
		Consent, justification and objection: A personal Information is processed because it is necessary for the

		conclusion or performance of a contract to which the Data Subject is party or for pursuing the legitimate interests of The University as a Responsible Party. **b.** The Data Subject may withdraw their consent, if consent was provided, to The University processing their Personal Information at any time provided that the lawfulness of the processing of Personal Information before such withdrawal, or the processing of Personal Information, will not be affected. **c.** The Data Subject may also object, at any time, to the processing of their Personal Information, by complying with the relevant process, and subject to there being reasonable grounds relating to their particular situation. **d.** The Data Subject is however forewarned that if they revoke consent or object to The University processing their Personal Information in terms of the POPIA, in circumstance where the processing of such Personal Information is necessary to carry out actions for the conclusion or performance of a contract, then the Data Subject may be excluded from any affected rights or benefits under the contract and, where such consent is operationally material to the continuation of the contract, that the relationship, undertaking, or arrangement, may have to be terminated, or suspended as the case be, for operational or otherwise legitimate reasons, to the extent as may be necessary. **e.** The University regards the processing of Personal Information as justifiable under the POPIA, which includes, processing that is necessary to carry out actions for the conclusion or performance of contractual relationships with Data Subjects, processing complies with an obligation imposed by law on The University, processing protects a legitimate interest of the Data Subject, processing is necessary for the proper performance of a public law duty by The University, or processing is necessary for pursuing the legitimate interest of The University or a third party to whom the information is supplied.

		f. The University has several policies and procedures that require or may result in the processing of personal information. In most instances the information is collected from the Data Subjects. The justification for processing will in most instances be based on either the conclusion and implementation of a contract or in order to comply with legislative or regulatory requirements. In all other instances where a Data Subject submits personal information or special personal information to The University pursuant to a policy or procedure it would be regarded as having consented to the processing of the said information for the purpose of implementing the policy or process.
		Collection from Data Subjects Personal information is collected directly from the Data Subject and also collected where contained in or derived from a public record or has deliberately been made public by the Data Subject.
		Collection from Other Sources Collection by the University may also take place when the Data Subject has: consented to the collection from another source, collection from another source would not prejudice a legitimate interest of the Data Subject, compliance would prejudice a lawful purpose of the collection, compliance is not reasonably practicable in the circumstances of the particular case, or, collection from another source is necessary for purposes of section 12 2 (d) of the POPIA. The University may make use of Operators who perform medical, credit and criminal vetting for The University subject to compliance with the POPIA.
Condition 3 Notification of collection and collection for specific purpose	**1.** The University processes Personal Information only for specific, explicitly defined and legitimate reasons, which purpose is communicated to the relevant Data Subject by way of privacy notices, as part of concluding agreements with The University, in this policy and other policies and procedures where such policies or procedures require or may result in the collection of Personal Information. **2.** The University complies with section 18 of the POPIA, in its reasonably practicable steps, by ensuring that Data Subjects are aware of the purpose of the processing of Personal Information.	Purpose for processing includes (but is not limited to) **a. Employee Candidates/Employees' Personal Information (including for academic staff):** which is processed to facilitate the employment relationship between the employee and The University. This Personal Information is processed on a continued and on-going basis throughout the duration of an employee's employment with The University for personnel management, administration, work and general business management, regulatory and statutory

	3. If The University is collecting information directly from a Data Subject, it will notify a Data Subject during the time of the collection. If however Personal Information is collected from another source, The University will apply a reasonable period of one-month within which to notify a Data Subject of the collection of information, unless a shorter period is practicable. **4.** The University is not entitled to notify a Data Subject in respect of the collection of Personal Information if it is justified to do so in compliance with section 18 of the POPIA.	compliance, and reporting. For example, The University requires the Personal Information for security purposes, to administer payroll, improve and maintain the administration of employee benefits (such as leave entitlement, facilitate the management of work and employees, operate performance and salary reviews, operate The University IT and communications systems, comply with record keeping and other legal obligations. After the termination of an employee's employment with The University, the Personal Information is processed to ensure the administration of post-employment benefits, if any and where applicable.
		b. Students/Prospective Students or Applicants /International Students Personal Information which is processed to facilitate the student relationship, or possible relationship, between the student and The University, in order for The University to provide a quality level of tertiary education. If a person in this category is under the age of 18 years and therefore falls to be a child in terms of legal requirements, the necessary consent from the parent or guardian must be obtained.
		c. Research Participants/Post-Doctoral Fellows, Alumni, Authors: which is processed to facilitate the relevant engagements in order to sustain or advance The University's academic activities.
		d. Governance and/or Appointed Office Bearers/External Members of Committees/ Council Members: which is processed to facilitate the engagements of such persons as arising from a constitutive or legislative document regulating such appointments.
		e. Suppliers' Personal Information: which is processed to facilitate the business relationship between the supplier / service provider and The University in order for the supplier / service provider to provide goods and/or services to The University as a customer.
		f. Keeping a record of processing activities: The University, in compliance with section 17 of the POPIA, will document

		processing activities, including in both written and electronic means, as to the various processing activities.
		g. Retention and restriction of records: The University has a retention and archiving policy that regulates the retention and archiving of information as required or authorised by law, as well as where such records are reasonably required for lawful purposes related to The University's functions and/or activities. The University takes reasonable measures to delete records of Personal Information or de-identify it as soon as reasonably practically possible after The University is no longer authorised to retain the records (as per relevant statutory and regulatory frameworks) or ensures appropriate safeguards are maintained in the event that Personal Information is retained for longer than statutory prescribed periods for historical, statistical or research purposes.
Condition 4 Further Processing Limitation	**1.** Personal Information is not processed for a secondary purpose unless that processing is compatible with the original purpose for processing. **2.** In this regard, The University complies with section 15 of the POPIA.	
Condition 5 Information Quality	**1.** The University takes reasonable steps to ensure that the Personal Information collected is complete, accurate, not misleading and updated where necessary and The University has regard to the purpose for which Personal Information is collected or further processed when taking such steps. **2.** In this regard, The University complies with section 16 of the POPIA. **3.** However, read with paragraph 5.3.5.1, Data Subjects are required to ensure that the Personal Information they provide is complete, accurate, not misleading and consistently updated where necessary.	
Condition 6 Openness	The University will take reasonable steps to ensure that the Data Subjects are aware of, amongst others, the Personal Information it collects and the purpose for which the Personal Information is processed. In this regard, The University complies with sections 17 and 18 of the POPIA.	
Condition 7 Security	**1.**The University secures the integrity and confidentiality of Personal Information that it	In order to give effect to clause 5.3.7.1, The

Safeguards	processes by taking appropriate, reasonable, technical and organisational measures to prevent: • loss of, damage to or unauthorised destruction of Personal Information; and • unlawful access to or processing of Personal Information.	University takes reasonable measures to: **a.**.identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control; **b.**.establish and maintain appropriate safeguards against the risks identified; **c.**.regularly verify that the safeguards are effectively implemented; and **d.**.ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
	The University complies with generally accepted information security practices and procedures which apply to it generally and also in terms of specific rules and regulations (where applicable) in respect of Universities **Operators.**	The University ensures compliance with sections 20 and 21 of the POPIA by entering into data processing agreements with Operators who process Personal Information for or on behalf of The University, thereby also ensuring that the Operator establishes and maintains the security measures referred to in section 19 of the POPIA.
	Notification of security compromises:	Although The University takes all reasonable measures to ensure the safety of the Personal Information that it processes, where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person or source, then The University will, as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of The University's information systems, notify the Information Regulator (in the manner prescribed by the POPIA) and the Data Subject (by e-mail to the Data Subject's last known e-mail address) of the alleged breach. The notification referred to in clause 5.3.7.5 shall include sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise.
Condition 8 **Data Subject Participation**	**1.** Access to personal information: A Data Subject may (subject to the provision of adequate proof of identity to The University) request to know whether their Personal Information is held by The University, as well as the	

	correction and/or deletion of any Personal Information held about them but The University may charge an access fee to cover the cost of retrieving the information and supplying it to a Data Subject. If The University and the Data Subject cannot reach agreement following The University's receipt of such a request, the Data Subject can ask The University to make a note of the requested correction alongside the information. **2.** In this regard, sections 23, 24 and 25 are applicable to Personal Information requests by Data Subjects. **3.** The Data Subject's access to Personal Information will need to adhere to the University's Manual on the Promotion of Access to Information that is readily available under the University's resources.	

Annexure B

1. Categorisation of Personal Information Processed

The University processes the following, but is not limited to, Personal Information of Data Subjects

DATA SUBJECT	PERSONAL INFORMATION PROCESSED
Students / Prospective Students or Applicants, International Students	Full names, identity number, students numbers, gender, race / B-BBEE information, age, language, education, financial information (such as creditworthiness and banking details), employment history, credit information, criminal information, references, physical and postal address, contact details (cellphone and e-mail address), pregnancy, marital status, physical or mental health, medical records, well-being, disability, religion, culture, language, birth, location, online identifiers, biometric and facial recognition information, photographs, breathalyser test results, vehicle registration, driver's license, birth and death certificates. If a person in this category is under the age of 18 years and therefore falls to be a child in terms of legal requirements, the necessary consent from the parent or guardian must be obtained.
Employment,candidates, employees, academic staff	B-BBEE/employment equity information, age, language, education, financial information (such as creditworthiness and banking details), employment history, credit information, criminal information, references, physical and postal address, contact details (cellphone and e-mail address), pregnancy, marital status, physical or mental health, medical records, well-being, disability, religion, culture, language, birth, location, online identifiers, biometric and facial recognition information, trade union membership, photographs, breathalyser test results, vehicle registration, driver's license, birth and death certificates, all Personal Information required for the administration of compensation and benefits (including payroll, promotions, salary increases, salary decreases, salary adjustments, bonuses, death benefit pay-outs, COIDA, disability), employee files (including performance records, disciplinary, CCMA records, employee grievances, formal written warnings, SHEQ), legal judgements, garnishee and other court orders
Research participants, post-doctoral fellows, alumni, authors	Full names, identity number, students numbers, gender, race / B-BBEE/employment equity information , age, language, education financial information (such as creditworthiness and banking details), employment history, credit information, criminal information, references, physical and postal address, contact details (cellphone and e-mail address), pregnancy, marital status, physical or mental health, medical records, well-being, disability, religion, culture, language, birth, location, online identifiers, biometric and facial recognition information, photographs, breathalyser test results, vehicle registration, driver's license, birth and death certificates.
Governance and/or appointed officer-bearers, external members of committees, council members	B-BBEE/employment equity information , age, language, education, financial information (such as creditworthiness and banking details), employment history, credit information, criminal information, references, physical and postal address, contact details (cellphone and e-mail address), pregnancy, marital status, physical or mental health, medical records, well-being, disability, religion, culture, language, birth, location, online identifiers, biometric and facial

	recognition information, trade union membership, photographs, breathalyser test results, vehicle registration, driver's license, birth and death certificates, all Personal Information required for the administration of compensation and benefits (including payroll, promotions, salary increases, salary decreases, salary adjustments, bonuses, death benefit pay-outs, COIDA, disability), employee files (including performance records, disciplinary, CCMA records, employee grievances, formal written warnings, SHEQ), legal judgements, garnishee and other court orders
Partner organisations, subsidiaries, donors and funders,	Name of legal entity or person, registration number or identity number, names of contact persons / directors / members and identifying documents such as identity document or passport of contact persons / directors / members, physical and postal address and contact details (email, cellphone), creditworthiness or other financial information, founding documents from the CIPC or other forms of proof of registration / incorporation such as trust deeds, partnership agreements or CC incorporation documents, tax related information, authorised signatories, resolutions for authority or business transactions, shareholding information, B-BBEE information, confidential correspondence, beneficiaries, ultimate beneficial owners, shareholding information, and any other Personal Information required for vetting purposes in terms of financial legislation such as FICA
Particular third parties: Different universities, government departments	Name of legal entity, registration number, names of contact persons / directors / members, physical and postal address, contact details (email, cellphone), financial and tax related information (tax clearance, tax pin, VAT number), founding documents (CIPC), authorised signatories, directors information for vetting purposes (criminal, credit and CIPC disqualification or deregistration), shareholding information, B-BBEE information, and any other Personal Information required for vetting purposes in terms of financial legislation such as FICA
Contractors / Suppliers / Service Providers: Juristic Persons	Name of legal entity, registration number, names of contact persons / directors / members, physical and postal address, contact details (email, cellphone), financial and tax related information (tax clearance, tax pin, VAT number), founding documents (CIPC), authorised signatories, directors information for vetting purposes (criminal, credit and CIPC disqualification or deregistration), shareholding information, B-BBEE information, and any other Personal Information required for vetting purposes in terms of financial legislation such as FICA
Contractor / Suppliers / Service Providers: Natural persons	Full names, identity number, gender, race / B-BBEE information, age, credit information, criminal information, references, physical and postal address, contact details (email, cellphone), financial and tax related information (tax clearance, tax pin, VAT number), and any other Personal Information required for vetting purposes in terms of financial legislation such as FICA
Beneficiaries in terms of Social Investment initiatives and community development	Name of legal entity, registration number, names of contact persons / directors / members and identifying documents such as identity document or passport of contact persons / directors / members, physical and postal address and contact details (email, cellphone), creditworthiness or other financial information, founding documents from the CIPC or other forms of proof of registration / incorporation such as trust deeds, partnership agreements or CC incorporation documents, tax related information, authorised signatories, resolutions for authority or business transactions, shareholding information, B-BBEE information, confidential

	correspondence, beneficiaries, ultimate beneficial owners, shareholding information, and any other Personal Information required for vetting purposes in terms of financial legislation such as FICA
Visitors, members of the public	Full names, identity number, physical and postal address, contact details (cellphone and e-mail address), vehicle registration, driver's license, biometric and facial recognition information.