PERSONAL INFORMATION PRIVACY POLICY

Reference number	1P_1.1.12
Responsible executive manager	Registrar
Policy owner	Registrar
Responsible division	Corporate and Information Governance Services
Status	Approved
Approved by	Council
Date of approval	17 June 2021
Review date	June 2025

Office of the Registrar

PERSONAL INFORMATION PRIVACY POLICY

Preamble

Against the background of the dream to be an internationally recognised university in Africa, distinguished for engaged scholarship, social responsiveness and an ethic of care, the Council of the North-West University (NWU) has adopted this Policy on 17 June 2021.

1 Interpretation and application

This Policy must be interpreted and applied in a manner consistent with, but not limited to –

1.1 Constitution of the Republic of South Africa, 1996;

1.2 Higher Education Act, 101 of 1997;

1.3 Protection of Personal Information Act, 4 of 2013 ("POPIA");

1.4 Promotion of Access to Information Act, 2 of 2000 ("PAIA")'

1.5 Statute of the North-West University ("the Statute")

1.6 Kink IV Report on Good Corporate Governance in South Africa;

1.7 POPIA Industry Code of conduct: Public Universities (adopted by the Board of Universities South Africa as guidelines on 24 June 2020);

1.8 Information Governance Framework of the NWU;

1.9 Research Ethics Policy of the NWU; and

1.10 all other applicable policies of the NWU.

2 Definitions

In this policy, unless the context indicates otherwise –

"automated means" refers to processing done by a computer;

"consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"data subject" means the person to whom the personal information relates, including –

- prospective students;
- student applicants;
- all registered students;
- exchange students;
- post-doctoral fellows;
- alumni;
- all NWU employees;
- employment candidates;
- external members of committees;
- researchers;
- research participants;
- authors;
- council members;
- service providers, suppliers, independent contractors;
- partner organisations;
- subsidiaries;

- donors and funders;
- visitors;
- members of the public;
- any other NWU stakeholder, where personal information is collected, processed or disposed of; and
- any other individual with whom the NWU may interact from time to time, whether or not such person is a natural or juristic person;

"de-identify" in relation to personal information of a data subject means to delete information that –

a) identifies the data subject;
b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
c) can be linked by a reasonably foreseeable method or other information that identifies a data subject, and de-identified had a corresponding meaning;

"filing system" refers to a structures set of personal information which is accessible according to specific criteria, regardless of whether it is centralised or decentralised, including anything from a physical file in an alphabetised filing cabinet to multiple inter-related databases that can be accessed from anywhere in the world and can handle complex search queries;

"information classification" means the process of assigning an appropriate level of classification to information to ensure that it receives an adequate level of protection;

"information governance" means the umbrella concept aiming at governing all information management activities that are performed to derive/ensure value from information for the NWU while complying with all regulatory requirements and international best practices;

"information management" entails the activities and organisational functions that are necessary in order to manage, control, and destroy data in any form regardless of their medium, origin and quality;

"information officer" means the vice-chancellor;

"Information Regulator" refers to the Regulator established in terms of section 39 of the POPIA;

"non-automated means" refers to a filing system other than a computer-accessible database;

"NWU employee" means an individual employed by the NWU on any basis, including full-time, part-time and fixed-term;

"operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"personal information" means personal information as defined in section 1 of the POPIA;

"Policy" means this Personal Information Privacy Policy;

"privacy impact assessment" is a structured approach for the NWU to understand the privacy risks associated with the processing of personal information and take appropriate steps to manage those risks;

"processing" means processing as defined in section 1 of the POPIA;

"special personal information" means special personal information as defined in section 1 of the POPIA;

"student" means a student as defined in paragraph 1 of the Statute;

3 Policy statement

The Council of the North-West University considers a proper process and framework for the management of the protection of privacy and provision of assurance to be of paramount importance for the good governance and effective management and administration of the North-West University, and therefore it is the policy of the North-West University to –

3.1 increase the level of the protection of privacy of information within the NWU by aligning the NWU's approach to information governance, specifically privacy, with that of the Information Regulator;

3.2 establish an environment to ensure the uniform and appropriate implementation of the POPIA to promote good information and technology governance to achieve the NWU's strategic objectives;

3.3 provide for the responsible use of personal information within the NWU.

4 Purpose

The purpose of this policy is to ensure, *inter alia*, the following:

4.1 *Data minimisation* – limiting the amount of personal information the NWU collects and retains.

4.2 *Transparency* – being open and honest about what personal information the NWU collects and how it will be used.

4.3 *Security* – protecting the personal information the NWU holds from harm.

4.4 *Use limitation* – ensuring that the NWU uses and discloses personal information only when necessary and lawfully.

4.5 *Privacy rights* – helping the NWU's data subjects to exercise their privacy rights and maintain control over their personal information.

5 Scope of application

This policy applies to –

5.1 all processing of personal information by "public higher education institutions" as defined in section 1 of the Higher Education Act, 101 of 1997;

5.2 all NWU employees and students who access, use or deal with personal information, or handle questions or complaints about personal information in the course of their NWU-related activities;

5.3 any individual who discloses personal information to the NWU, whether they are part of the NWU community or any member of the public worldwide;

5.4 personal information collected by the NWU in connection with the services it offers, whether it be personal information collected offline or online; and

5.5 personal information collected from operators' websites or platforms.

6 Roles, responsibilities and accountability

6.1 Information officer

6.1.1 The Information Officer of the NWU is the Vice-Chancellor.

6.1.2 The duties and responsibilities of the information officer must be performed in accordance with section 55 of the POPIA and the designation of deputy information officers and delegation of duties and responsibilities to them must be performed in accordance with section 56 of the POPIA and section 17 of the PAIA.

6.1.3 The information officer must be registered with the Information Regulator.

6.1.4 Deputy information officers may be appointed to assist the information officer with his/her duties.

6.2 The Technology and Information Governance Committee

The Technology and Information Governance Committee of Council must advise the Council regarding its statutory governance responsibility to nurture a culture at the NWU that values, protects and utilises information in an optimal way and which will result in the protection of the privacy of personal information.

6.3 NWU Management Committee (UMC)

6.3.1 On the advice from the Information Management Committee the UMC must fulfil a management role regarding the protection of the privacy of personal information in alignment with the direction set by the council.

6.3.2 The UMC has the obligation to –

- promote a nurturing culture and embedding the protection of the privacy of personal information in decision-making and business processes;
- establish procedures and standards to ensure compliance to NWU policies and rules;
- create awareness of and ensure compliance with legal, regulatory and other obligations; and
- to keep the Technology and Information Governance Committee informed of matters relevant o privacy of personal information.

6.4 Information Management Committee (IM Committee)

The IM Committee, in accordance with the principles laid down in the NWU Information Governance Framework advises the UMC on –

6.4.1 compliance with relevant international and national regulations, legislation and directives; and

6.4.2 the implementation of the NWU Information Governance Framework and the development of policies and rules providing for the execution of the Framework.

6.5 NWU employees

6.5.1 Responsibility for the day-to-day administration of and compliance with this policy is the responsibility of line managers, who must ensure that employees -

6.5.1.1 actively seek to understand the privacy risks, controls and obligations that relate to activities relevant to the work environment;

6.5.1.2 support and participate in establishing a culture of the protection of privacy of personal information;

6.5.1.3 undertake activities in compliance with legislation and NWU policies and procedures; and

6.5.1.4 report new risks, breaches and weaknesses of controls to the relevant line manager, and as required under NWU policies.

6.5.2 All employees have the responsibility to –

6.5.2.1 ensure that their personal information is updated continuously;

6.5.2.2 adhere to the relevant information governance and management standards, policies and procedures; and

6.5.2.3 ensure that they attend the POPIA training and awareness sessions regularly and repeat such training at least once every four years.

6.5.3 All newly appointed employees have the responsibility to attend a POPIA training session within three (3) months after accepting employment with the NWU.

6.6 NWU students

All students have a responsibility to –

6.6.1 protect personal information and other NWU information and adhere to the relevant information governance and management standards, policies and procedures; and

6.6.2 ensure that their personal information is updated continuously.

6.7 NWU Council members and members of Council Committees

All NWU Council members and members of Council Committees have a responsibility to protect and keep confidential personal information that is shared from time to time as part of the proceedings of the Council and its committees.

7 Procedures and guidelines

The information officer may prescribe procedures and guidelines relevant to the implementation of this policy, including for –

7.1 collection of information;

7.2 processing of information;

7.3 storage of information;

7.4 disposal of information;

7.5 anonymization;

7.6 incident planning and response;

7.7 standard operating procedures for high-level and operational privacy impact assessments;

7.8 the types of personal information the university must collect and maintain for its purposes.

8 Information processing conditions

The conditions prescribing the minimum threshold requirements for the lawful processing of personal information by the NWU are provided for in section 4 and Part A of Chapter 3 of the POPIA.

9 Information classification

The NWU must –

9.1 establish a framework for the classification of information for the purposes of maintaining the required level of protection of personal information;

9.2 distinguish personal information from other information that is vital for POPIA compliance;

9.3 have a process to identify and keep on record all personal information in its possession; and

9.4 distinguish personal information from special personal information.

10 Retention of personal information

10.1 The NWU must apply a records management policy which provides for a file plan and disposal schedule that details the retention of personal information and the disposal thereof.

10.2 Personal information that is stored by the NWU in an electronic medium must be protected from unauthorised access by a password management system.

10.3 Personal information in hard-copy (paper-based) must be stored in a safe and secure storage area in the NWU department that uses the information.

10.4 The NWU may not retain a data subject's personal information longer than necessary to achieve the purpose for which the information was collected or as contemplated in the NWU file plan and disposal schedule, whichever timeframe is the shortest.

10.5 If it is no longer necessary to keep personal information for any reason, the NWU must take reasonable steps to destroy, delete or de-identify the information according to approved and documented procedures, rendering the data permanently irretrievable.

11 Verification or updating personal information from sources other than the data subject

The NWU may verify the accuracy of personal information and update such information in large batches, by comparing the information with publicly available information.

12 Information security breach notification

The information officer must report unauthorised access to, or acquisition of personal information by an unauthorised person to the Information Regulator and to data subjects and must ensure such breaches are kept on record.

13 Research activities

13.1 The NWU must ensure that its research activities comply with the provisions o the POPIA if it involves identifiable personal information.

13.2 For purposes of complying with the POPIA, the NWU must –

- establish and maintain a research data management procedure;
- develop a privacy impact assessment to identify research projects which have critical privacy implications for research participants;
- ensure that both the research data management procedure and privacy impact assessment are implemented via existing research ethics approval processes;
- ensure that all principal investigators complete certified training in research data management and privacy; and
- ensure that other researchers complete awareness training in research data management and privacy.

13.3 Insofar as exceptions regarding retention, notification and processing of personal information are allowed by the POPIA for the purposes of research, the NWU must regulate such exceptions in its research data management policy and set of procedures.

14 Information sharing with third parties

14.1 The NWU must take reasonable steps to ensure that personal information is not disclosed to third parties except in certain circumstances, including where –

14.1.1 there is a legal justification for the release of the information;

14.1.2 the individual has consented to the release;

14.1.3 the release of the information is a condition of a student's sponsorship or enrolment;

14.1.4 the NWU is authorised or required by law or regulatory requirements to disclose the information;

14.1.5 the NWU is required by any contract to disclose the information; or

14.1.6 the information is provided to a third party that provides services to the NWU in alignment with its core function, in which case the NWU will ensure that the service provider agrees to preserve the confidentiality or personal information (an information sharing agreement can be drafted in these cases) is required.

14.2 The NWU must take legal requirements and exceptions pertaining to the sharing of personal information with third parties not provided for in the POPIA into consideration.

15 Cross-border transfer of information

The NWU may provide personal information outside of South Africa, subject to the restrictions provided for in South African and foreign legislation.

16 Direct marketing

16.1 Prospective students, registered students, and alumni will have the ability to 'opt-in' or 'opt-out' to an opportunity if they wish to be contacted or involved further;

16.2 The data subject will always be able to unsubscribe in subsequent communications.

17 Privacy Impact Assessments (PIAs)

The NWU must develop privacy impact assessments and a procedure to ensure that the assessments are performed.

18 E-mail management

The NWU must –

18.1 take reasonable steps to ensure that sensitive personal information is not sent by email; and

18.2 mandate the use of a standard email disclaimer to be applied to all outgoing emails from the NWU.

19 Awareness and training

The NWU must –

19.1 develop an awareness programme and training programme, methods and procedures and implement to monitor and maintain the POPIA programme;

19.2 ensure that employees are made aware of the regulations, policies and procedures continuously; and

19.3 require all employees to attend compulsory POPIA awareness training sessions as contemplated in paragraph 6.5.2.3 and 6.5.3 of this policy.

Original details: (11664754) P:\Policies\2021\1P_1.1.12\Personal Information Privacy Policy.docm
2 July 2021

File reference: 1P_1.1.12_2021