school of government
Department:
National School of Government
REPUBLIC OF SOUTH AFRICA

THE NATIONAL SCHOOL OF GOVERNMENT'S (NSG's) POLICY ON THE PROTECTION OF PERSONAL INFORMATION (POPI)

VERSION AND AMENDMENT SCHEDULE

Version	Version Date	Author	Description of Amendments
Original Ver 1.0	27 February 2023	Mr. Given Mditshwa	New Policy

APPROVAL AND CONTROL SCHEDULE

Approved by	Designation	Responsibility	Signature	Date Approved	Copy Status
Mr. Given Mditshwa	D: Legal Services	Policy Drafter		27/02/23	Master
Mr. Tau Nyaku	Deputy Information Officer	Process Owner		27/2/2023	
Mr. Rufus Nchabeleng	Deputy Information Officer	Process Owner		27/02/2023	
Ms. Lakela Kaunda	DDG: Administration	Supporting Authority		28/02/2023	
Prof. Busani Ngcaweni	Principal	Approving Authority		01/03/2023	

1. INTRODUCTION

1.1 The National School of Government is a national Government Department that is obligated to comply with the Protection of Personal Information Act 4 of 2013 ("POPIA" or the Act). It is therefore on the basis of POPIA that the National School of Government has drafted this policy on the protection of personal information.

1.2 POPIA requires the National School of Government to inform its employees and clients as to how their personal information is collected, used, disclosed and destroyed.

1.3 The National School of Government guarantees its commitment to protecting its employees and clients' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

1.4 This Policy sets out how the National School of Government deals with its employees' and clients' personal information and in addition for what purpose the said information is used. This policy is made available on the Department's website at www.thensg.gov.za and on request to either the Information Officer (IO) and or the Deputy Information Officers (DIOs).

1.5 This Policy is drafted in compliance with Chapter 3 of the POPIA which requires that "Personal Information may only be processed if given the purpose for which it is processed, it is adequate, relevant and not excessive." The National School of Government collects and processes employees' and clients' personal information pertaining to the employees' conditions of service and employees' and clients' education and training needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, the National School of Government will inform the employees and clients what personal information they are required to provide and what information is optional.

1.6 The National School of Government also collects and processes employees' and clients' personal information for marketing purposes to ensure that its courses and services remain applicable to its existing and potential employees and clients.

1.7 This policy should be read together with the National School of Government's Records Management policy and any other information management policy applicable to the National School of Government from time to time.

2. DEFINITIONS

In this policy, unless the context indicates otherwise-

"**Biometrics**" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid (DNA) analysis, retinal scanning and voice recognition;

"**Child**" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning himself or herself;

"**Competent person**" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

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

"**Constitution**" means the Constitution of the Republic of South Africa, 1996;

"**Data subject**" means the person to whom personal information relates;

"**De-identify**", in relation to personal information of a data subject, means to delete any 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 to other information that identifies the data subject, and "**De-identified**" has a corresponding meaning;

"**Direct marketing**" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

(a) promoting or offering to supply, in the ordinary course of business, any goods

or services to the data subject; or
(b) requesting the data subject to make a donation of any kind for any reason;

"Electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"Filing system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"Information matching programme" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"Information officer" of, or in relation to, a—
(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17 of the Act;

"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;

"Person" means a natural person or a juristic person;

"Personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, 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;

"Processing" means any operation or activity or any set of operations, whether or not 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 information;

"Public body" means—
(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
(b) any other functionary or institution when—
(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
(ii) exercising a public power or performing a public function in terms of any legislation;

"Public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"Record" means any recorded information—
(a) regardless of form or medium, including any of the following:

(i) writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

"Regulator" means the Information Regulator established in terms of section 39 of the Act;

"Re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, 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 to other information that identifies the data subject, and "**re-identified**" has a corresponding meaning;

"Republic" means the Republic of South Africa;

"Responsible party' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"Special Personal Information" means personal information as referred to in section 26 of the Act;

"This Act" includes any regulation or code of conduct made under the Protection of Personal Information Act No.4 of 2013; and

"Unique identifier" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3. PERSONAL INFORMATION COLLECTED

3.1 Chapter 3 of POPIA states that Personal Information –

(a) must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject;

(b) may only be processed if given the purpose for which it is processed, it is adequate, relevant and not excessive;

(c) may further be processed subject to compliance with sections 11, 12 and 13 of POPIA, namely relevant consent, justification and collection directly from the date subject except as is otherwise provided in the Act.

3.2 The National School of Government collects and processes employees' and clients' personal information pertaining to the employment relationship in the case of employees or employees' and clients' registration, education and training needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, the NSG will inform the employee or the client what information is required and what information is optional. Examples of personal information that the NSG collects include but is not limited to:

a) Employees' or clients' identity number, persal number, title, name, surname, home and work addresses, banking details, educational information, postal code, marital status, contact details being telephone number and e-mail address, employer details, company or organisation name and registration number and how many dependents they have; and

b) Any other information required by the NSG or its partners in order to provide employees' with an accurate analysis of their employment status or

employees' and clients' with education and training registration requirements or course enrolment and progress status reports

3.3 The National School of Government also collects and processes employees' and clients' personal information for marketing purposes to ensure that NSG courses and services remain applicable to existing and potential employees and clients.

3.4 The NSG is obliged to have agreements in place with all its partners and third-party Service Providers to ensure that there is a mutual understanding with regard to the protection of clients' personal information. The NSG's partners will be subjected to similar data privacy and personal information policies that are relevant to them.

3.5 With employees' and clients' consent, the NSG may also supplement the information provided with information it receives from other providers or partners in order to offer a more consistent and personalised experience in client's course enrolment with the NSG. For purposes of this Policy, clients included potential and existing clients.

4. HOW PERSONAL INFORMATION IS USED

4.1 Employees' and clients' personal information will only be used for the purpose for which it was collected and agreed to.

4.2 This may include:

4.2.1 Providing courses or services to employees and clients and to carry out the transactions requested including course progress and completion status, attendance records and so on;

4.2.2 For registration purposes:

(a) Assessing and processing Learner registration forms;
(b) Conducting reference searches or verification;
(c) Confirming, verifying and updating client details;
(d) The way training will be conducted, that is either virtually, online or face-to-face.

4.2.3 For purposes of registration history:

(a) For the detection and prevention of fraud, crime or other malpractices;

(b) Conducting market or customer satisfaction research;

(c) For audit and record keeping purposes;

4.2.4 In connection with legal proceedings:

(a) Providing services to employees and clients to carry out the services requested and to maintain and constantly improve the relationship;

(b) Providing communications in respect of National School of Government and regulatory matters that may affect employees and or clients; and

4.3 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

4.4 According to section 10 of POPIA, personal information may only be processed if certain conditions are met which conditions are listed below along with supporting information for the National School of Government's processing of personal information:

(a) Client consents to the processing - consent is obtained from employees' and clients' during the introductory, appointment and registration analysis stage of our relationship;

(b) The processing is necessary in order to conduct an accurate analysis of employees' and or clients' needs for purposes of amongst others, application and registration for a course, award or conferment of a certificate or a diploma;

(c) Processing complies with an obligation imposed by law on the National School of Government;

(d) Processing protects a legitimate interest of an employee or the client - it is in the employees' or client's best interest to have a full and proper application and registration analysis performed in order to confirm whether to provide the employee or the client with an applicable service or determine whether the employee or the client qualifies to register for a particular course and this requires obtaining personal information;

(e) Processing of course completion status for reporting back to the employer who paid for the course;

(f) Processing is necessary for pursuing the legitimate interests of National School of Government.

5 DISCLOSURE OF PERSONAL INFORMATION

5.1 The NSG may disclose employees' and client's personal information to any of the other Government Department/s, organs of state and or approved third-party Service Providers whose services or courses the employees' and or clients' elect to use. The NSG shall enter into agreements to maintain confidentiality and ensure that such Government Department/s, organs of state and or approved third-party Service Providers comply with confidentiality and privacy conditions.

5.2 The NSG may also disclose employees' and clients' information where the NSG has a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect our rights.

6 SAFEGUARDING EMPLOYEES AND CLIENTS INFORMATION

6.1 It is a requirement of POPIA to adequately protect the personal information that the National School of Government holds and to avoid unauthorized access and use of employees' or clients' personal information. The National School of Government will continuously review its security controls and processes to ensure that employees' and clients' personal information is secure.

The following procedures are in place to protect Personal Information:

(a) The Information Officer whose details appear on the NSG's website and elsewhere in this policy, is responsible for compliance with the conditions of the lawful processing of Personal Information and other provisions of POPI. The Information Officer is assisted by two Deputy Information Officers whose details also appear on the NSG's website and elsewhere in this policy;

(b) This Policy has been put in place throughout the National School of Government;

(c) Each new employee will be required to sign an employment contract and or a POPIA pledge and acknowledgment containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI. Similarly, clients will sign Learner registration forms containing consent clauses relevant to the use and storage of clients personal information, marketing purposes or any other action so required, in terms of POPIA;

(d) Every person in the employ of the National School of Government at the time that this policy is approved will be required to sign an addendum to his or her Employment Contract and or a POPIA pledge and acknowledgment containing relevant consent clauses for the use and storage of his or her personal information, marketing purposes or any other action so required, in terms of POPIA;

(e) The National School of Government's archived clients' and employees' information is stored on site and in the offices of the State Information Technology Agency (SITA) which is also governed by POPIA;

(f) The National School of Government's partners and other third-party Service Providers will be required to sign a Service Level Agreement or other contract guaranteeing their commitment to the Protection of Personal Information;

(g) The National School of Government will introduce an Electronic Document Management System (EDMS) whereby NSG'S hard copy files are to be captured electronically for back up purposes. All files will be archived at the National School of Government's Disaster Recovery Site (DRS) which will be available both electronically and in hard copy format;

(h) All electronic files or data are backed up by the Department's Information & Communications Technology (ICT) Unit which is responsible for system security which protects against third-party access and physical threats. The Department's ICT unit is responsible for electronic information security;

(i) Consent to process information is obtained from employees and clients (or a natural or juristic person who has been given authorization from the client to provide the clients Personal Information) during the introductory, appointment and needs analysis stage of the employment or education and training relationship.

7 ACCESS AND CORRECTION OF PERSONAL INFORMATION

7.1 Employees' and clients' have the right to access the personal information that the National School of Government holds about them. To request information, employees and clients will have to complete the relevant Promotion of Access to Information Act (PAIA) form. The NSG may at its sole discretion require proof of identity or proof of authority in order to satisfy itself that it is dealing with the correct data subject or other authorised person.

7.2 Employees and clients also have the right to request the National School of Government to update, correct or delete their Personal Information on reasonable grounds.

7.3 Once a client objects to the processing of their personal information, the National School of Government may no longer process the said Personal Information. The National School of Government will take all reasonable steps to confirm the employees' or clients' identity before providing details of their personal information or making changes to their personal information.

7.4 The details of the National School of Government's Information Officer, Deputy Information Officers and the Head Office are as follows:

7.4.1 **DETAILS OF THE INFORMATION OFFICER (IO)**

Prof. Busani Ngcaweni
The Principal
ZK Matthews Building
70 Meintjies Street
Sunnyside
PRETORIA
0001
Telephone Nos. (012) 441 6033/6000
Telefax No. 086 660 8812
E-mail: dg.secretary@thensg.gov.za
Website: www.thensg.gov.za

7.4.2 DETAILS OF DEPUTY INFORMATION OFFICERS (DIOs)

7.4.2.1 Mr. Rufus Nchabeleng

Director in the Office of the Principal
ZK Matthews Building
70 Meintjies Street
Sunnyside
PRETORIA
0001
Telephone Nos. (012) 441 6033/6000
Telefax No. 086 660 8812
E-mail: Rufus.Nchabeleng@thensg.gov.za
Website: www.thensg.gov.za

7.4.2.2 Mr. Tau Nyaku

Director: Workplace Environment
ZK Matthews Building
70 Meintjies Street
Sunnyside
PRETORIA
0001
Telephone Nos. (012) 441 6851/6000
E-mail: Tau.Nyaku@thensg.gov.za
Website: www.thensg.gov.za

7.4.3 HEAD OFFICE DETAILS

The National School of Government
ZK Matthews Building
70 Meintjies Street
Sunnyside
PRETORIA
0001
Telephone Nos. (012) 441 6000 and 0861 008 326
Telefax No. 086 660 8812
Website: www.thensg.gov.za

8 DESTRUCTION OF DOCUMENTS

8.1 Documents should be destroyed or deleted after the termination of the retention period prescribed by law or the code of conduct or de-identified when they are no longer needed. The destruction or deletion of a record of personal information aforesaid must be done in a manner that prevents its reconstruction in an intelligible form.

8.2 The National School of Government's Records Management Unit or other authorised unit will attend to the destruction of the documents in line with relevant and applicable legislation and processes.

9 NON-COMPLIANCE WITH THE POLICY

Non-compliance with the National School of Government's policy on the protection of personal information will result in a disciplinary process for employees or registration services for clients not to be processed; and if processed already then to deregistration and or the imposition of penalties stated in section 107 of the POPIA whichever is most appropriate in the circumstances.

10 EFFECTIVE DATE OF THE POLICY

This policy shall be effective from the date of signature by the Principal or other duly authorized official.

11 REVIEW OF THE POLICY

This policy shall be reviewed every 5 (five) years from date of signing or as and when the need arises. Should the policy not be reviewed, the current policy shall apply until reviewed.

PROF. BUSANI NGCAWENI
PRINCIPAL
DATE: 01/03/2023