KWAZULU-NATAL PROVINCE
COMMUNITY SAFETY AND LIAISON
REPUBLIC OF SOUTH AFRICA

PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)
COMPLIANCE POLICY FRAMEWORK

TABLE OF CONTENTS

1 DEFINITIONS

1.1 ‘‘**Automated means**’’ means any equipment capable of operating automatically in response to instructions given for the purpose of processing information;

1.2 “**Data Subject**” means the person to whom personal information relates;

1.3 “**Department**” means the KwaZulu-Natal Department of Community Safety and Liaison;

1.4 “**Deputy Information Officer**” means an official of the Department appointed by the Head of Department in terms of PAIA and POPIA;

1.5 “**Information Officer**” means the Head of Department;

1.6 “**operator**” means a person who processes personal information for the Department in terms of a contract or a mandate;

1.7 “**PAIA**” means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

1.8 “**PERSAL**” means the personnel salary administration system of the public service in South Africa;

1.9 “**person**” means a natural person or a juristic person;

1.10 “**personal information**” means information relating to any data subject as defined in POPIA including but not limited to views or opinions of another individual about the data subject; and information relating to such data subject’s -

a) race, sex, gender, sexual orientation, pregnancy, marital status, nationality, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, conscience, belief, cultural affiliation, language and birth;
b) education, medical, financial, criminal or employment history;
c) names, identity number and/or any other personal identifier, including any numbers which may uniquely identify a data subject, account or client number, password, pin code, customer or data subject code or number, numeric, alpha or alpha-numeric design or configuration of any nature, symbol, e-mail address, domain name or IP address, physical address, cellular phone number, telephone number or other particular assignment;
d) blood type, fingerprint or any other biometric information;
e) personal opinions, views or preferences;

f) correspondence that is implicitly or expressly of a personal, private or confidential nature (or further correspondence that would reveal the contents of the original correspondence); and

g) corporate structure, composition and business operations (in circumstances where the data subject is a juristic person) irrespective of whether such information is in the public domain or not;

1.11 "**POPIA**" means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013);

1.12 "**processing or processed**" 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, testing of or use;

b) dissemination by means of transmission, distribution or making available in any other form by electronic communications or other means; or

c) merging, linking, blocking, degradation, erasure or destruction;

1.13 "**Regulator**" means the Information Regulator contemplated in PAIA and POPIA;

1.14 "**requester**" means any person making a request for access to a record of the Department;

1.15 "**Responsibility Manager**" means a manager of the department responsible for a directorate within the department;

1.16 "**special personal information**" means personal information concerning –

1.16.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

1.16.2 the criminal behaviour of a data subject to the extent that such information relates to –

a) the alleged commission by a data subject of any offence; or

b) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings;

1.17 "**SITA**" means the State Information Technology Agency.

2 AUTHORITY

POPIA was assented to on 26 November 2013 and came into operation, in the main, on 1 July 2020.

The purpose of POPIA is, amongst others, to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party. POPIA applies to the processing of personal information entered in a record by or for the Department by making use of automated or non-automated means provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

Chapter 3 of POPIA regulates the processing of personal information by or for a responsible party through compliance with the eight conditions for the lawful processing of personal information, the processing of special personal information and the processing of personal information of children.

A compliance framework is a requirement of the Regulations in terms of POPIA. This Compliance Policy Framework is approved for application in the Department in pursuance of this obligation.

3 INFORMATION AND DEPUTY INFORMATION OFFICERS

3.1 Information Officer

Section 55(1) and Regulation 4 of POPIA set out the duties and responsibilities of an Information Officer, which include the following:

3.1.1. the encouragement of compliance by the Department with the conditions for the lawful processing of personal information. For example an Information Officer may develop a policy on how employees should implement the eight conditions for the lawful processing of personal information or consider issuing a circular in the case of provincial and national departments;

3.1.2. dealing with requests made to the Department pursuant to POPIA. For example an Information Officer of a Department will be expected to render such reasonable assistance, free of charge, as is necessary to enable the requester or data subject to comply with the prescribed process for

submitting a request in terms of section 18 of PAIA and section 24 of POPIA. If a requester or data subject has made any request that does not comply with the requirements of PAIA or POPIA, the Information Officer concerned may not refuse the request because of

3.1.3. that non-compliance, unless the Information Officer has-

a) notified the data subject or requester of his/her intention to refuse the request and stated in the notice, the reasons for the contemplated refusal, as well as his/her availability to assist that requester or data subject to remove the grounds for refusal;

b) given the requester or data subject a reasonable opportunity to seek such assistance;

c) as far as reasonably possible, furnished the requester or data subject with any information that would assist the making of the request in the prescribed form; and

d) given the requester a reasonable opportunity to confirm the request or alter it to comply with section 18 of PAIA or 24 of POPIA.

3.1.4. working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA in relation to the Department.

3.1.5. otherwise ensuring compliance by a Department with the provisions of POPIA. For example POPIA prescribes eight conditions for the lawful processing of personal information by or for a responsible party and it is the responsibility of the Information Officer to ensure compliance with those conditions.

3.1.6. ensure that a compliance framework is developed, implemented, monitored and maintained;

3.1.7. a personal information impact assessment is done to ensure that adequate

3.1.8. measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

3.1.9. an information manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA;

3.1.10. internal measures are developed together with adequate systems to process requests for information or access thereto;

3.1.11. internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator; and

3.1.12. annually, and in terms of section 32 of PAIA, submit to the Regulator a report regarding PAIA requests for access to information received and processed.

3.2 Deputy Information Officer

3.2.1 Section 17 of PAIA provides for the designation of a Deputy Information Officer of a public body.

3.2.2 In order to render the Department as accessible as reasonably possible the Information Officer must designate one or more Deputy Information Officers as are necessary, depending on the structure and size of the Department.

3.2.3 Only employee(s) of the Department may be designated as a Deputy Information Officer.

3.2.4 A designation to a Deputy Information Officer must be in writing.

3.2.5 A Deputy Information Officer should have a reasonable understanding of POPIA and PAIA and the business operations and processes of the Department in order to execute his or her duties.

3.2.6 A Deputy Information Officer should have a reasonable understanding of the Department. An employee(s) with institutional knowledge is preferred for designation as a Deputy Information Officer(s).

3.2.7 Only an employee of the Department can be delegated as a Deputy Information Officer.

3.2.8 The delegation of any powers or duties and responsibilities to a Deputy Information Officer does not prohibit an Information Officer from exercising the powers or performing the duty that he or she has delegated to a Deputy Information Officer.

3.2.9 The Department must, if necessary, update the particulars of an Information Officer and Deputy Information Officer(s) at intervals of not more than one year.

4 CONDITIONS FOR LAWFUL PROCESSING

When processing personal information of any person, the department must ensure that the processing complies with the following eight conditions for lawful processing of personal information:

4.1. Accountability – the Department must take overall responsibility to ensure that it processes personal information lawfully.

4.2. Process limitation – the Department may only process such information that it reasonably needs to process for purposes of executing its mandates. A person may at any stage object to the processing of his or her personal information. If a person objects, then the Department may no longer process that person's personal information.

4.3. Purpose specification – the Department can only process the personal information of a person for purposes directly related to the object and purpose of the Department's mandate.

4.4. Further processing limitation – any further processing of the personal information of persons must be compatible with the purpose for which the information was originally obtained.

4.5. Information quality – the Department must take practical reasonable steps to ensure that personal information it processes is correct, up to date and complete.

4.6. Openness – a person must be notified that his or her personal information is being processed by the Department. The Department must also document all processing transactions through filing registers, document movement registers and transaction reports.

4.7. Security safeguards – the Department must put in place adequate security measures and controls to safeguard the personal information of persons against loss, damage and misuse. The Department must notify the Regulator and an affected person of any security breach.

4.8. Data subject participation – the Department must, upon request by a person confirm whether it is processing the personal information of that person. It must also correct, destroy and/or delete the personal information of a person upon request.

To further summarise, personal information must be obtained fairly and lawfully; used only for the specified purpose for which it was originally obtained; adequate, relevant and

processing may not be excessive to purpose; accurate and up to date; accessible to the data subject; kept secure; and destroyed after its purpose is completed.

5 CONSENT

It is not necessary for the Department to obtain consent from a data subject to process his or her personal information, when:

5.1 processing complies with the obligation imposed by law on the responsible party;

5.2 processing protects a legitimate interest of the data subject;

5.3 processing is necessary for the proper performance of a public law duty by the Department;

5.4 processing is necessary for pursuing the legitimate interests of the Department or of a third party to whom the information is supplied.

6 COLLECTION FOR A SPECIFIC PURPOSE

The Department must collect personal information of a data subject for a specific purpose, which in this context is for –

6.1 human resource management relating to applicants for employment and employees;

6.2 recruitment, deployment and payroll management of crime prevention volunteers;

6.3 financial and supply chain management relating to suppliers, service providers and assets;

6.4 fleet management relating to the use of official vehicles;

6.5 security management relating to building access control and maintenance of security at offices;

6.6 information technology management relating to users of the system and equipment;

6.7 monitoring and evaluation of police service delivery;

6.8 investigation of complaints of poor police service delivery;

6.9 promoting community police partnerships through support provided to community safety structures;

6.10 facilitating the resolution of inter- and intra-community conflicts;

6.11 undertaking community safety related research;

6.12 community engagement on community safety related issues;

6.13 internal planning, monitoring and evaluation of performance of the Department.

7 RETENTION AND RESTRICTION OF RECORDS

7.1. The Department must not retain records of personal information of data subjects for longer than authorised to achieve the purposes specified in paragraph 6 hereof, unless such information is required for historical, statistical or research purposes and provided that adequate safeguards are in place.

7.2. The Department must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the Department is no longer authorised to retain the record.

7.3. The destruction or deletion of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

8 INTEGRITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

8.1. All employees of the department and all crime prevention volunteers must protect the integrity of personal information and treat personal information as confidential.

8.2. In order to secure the integrity and confidentiality of personal information collected, the Department must take appropriate, reasonable technical and organisational measures to prevent the loss or damage to or unauthorised access of personal information. In this regard, Responsibility Managers and District Coordinators must ensure that personal information held by their directorates / within their offices is retained in secure facilities subject to strict access protocols.

8.3. An employee or volunteer must immediately report any unauthorised access of personal information of a data subject to the Responsibility Manager / District Coordinator concerned who in turn must report same to the Deputy Information Officer.

9 SPECIAL PERSONAL INFORMATION

9.1. Although the Department is not allowed to process special personal information of a data subject, the Department may process special personal information of a data

subject, if such processing is necessary for the proper functioning of the Department and –

a) processing is carried out with the consent of a data subject;
b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;
c) processing is necessary to comply with an obligation of international public law;
d) processing is for historical, statistical or research purposes;
e) information has deliberately been made public by the data subject;
f) processing is necessary for the implementation of provisions of laws, pension regulations or collective agreements;
g) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity;
h) to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

9.2. An employee may only process special personal information subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Department and a data subject.

10 PERSONAL INFORMATION CONCERNING A CHILD

The Department may not process personal information concerning a child, unless prior consent of a competent person has been obtained.

11 ACCESS TO PERSONAL INFORMATION

The Department must upon request confirm whether or not it holds personal information about a data subject. Any request must be submitted to the Deputy Information Officer for processing in accordance with this policy.

12 PERSONAL INFORMATION PROCESSED BY DEPARTMENT

The categories of personal information processed by the Department are contained in Annexure A, which specifies the Processing Component, Data Subjects, Personal

Information Processed, Processing Purpose, Collection Origin, Processes, Record Formats, Disposal of Records and Authority for Processing.

13 OPERATORS

13.1. An operator must only process personal information with the knowledge or authorisation of the Department, treat such information as confidential, and only disclose such information if required to do so by law, or in the course of the proper performance of its duty.

13.2. The Department must enter into a written contract with an operator to ensure that the operator establishes and maintains appropriate, reasonable, technical and organisational security measures when processing personal of data subjects.

13.3. In the event of a unathorised access to the system of the operator, such an incident should be reported immediately to the Department by the operator.

14 DUTIES OF ALL UNITS, DIRECTORATES AND OFFICES

14.1. Maintain Personal Information Inventory for the unit / directorate / office

14.2. Ensure physical and technical security measures are taken to safeguard personal information kept in cabinets and on information technology equipment / systems

14.3. Password-protect all electronic files containing personal information. The passwords to files must be recorded in a register which is stored in a secured space

14.4. De-identify personal information as soon as possible

14.5. Adhere to Records Management Policy

14.6. Review meeting attendance registers to ensure that only essential personal information is collected

15 DUTIES OF CORPORATE SERVICES

15.1 Human Resources

15.1.1. Comply with Provincial or National Policy / Procedure on PERSAL and human resource management in respect of personnel information security and record management

15.1.2. Ensure that POPIA notices are contained in post advertisements and are included in application forms

15.1.3. Ensure that POPIA notices are sent to any new appointees and contained in personal information request forms

15.1.4. On an annual basis validate existing personal information of employees

15.1.5. Ensure POPIA awareness is included in any staff induction programmes

15.1.6. Continuously review the need for prior authorisation from the Regulator in respect of financial vetting processes and advise the Information Officer accordingly

15.2 Auxiliary Services

15.2.1. Ensure physical and technical security measures are taken to safeguard personal information kept by Registry

15.2.2. Ensure adequate business continuity measures are in place to protect personal information records from unintended destruction or loss

15.2.3. Adhere to and administer the Records Management Policy

15.2.4. Annually review the Records Management Policy and procedures to ensure compliance with POPIA

15.2.5. Ensure the display of POPIA notices at building entrances

15.3 Information Technology

15.3.1. Provide support and guidance to employees in respect of technical measures to safeguard personal information stored on information technology equipment / systems

15.3.2. Assist employees of the department De-identify personal information in respect of personal information stored on information technology equipment / systems

15.3.3. Assist the Director: Corporate Services in respect of the destruction of electronic records of personal information

15.3.4. Annually review the IT policy and framework of the department to ensure alignment with POPIA

15.3.5. Annually review the electronic data storage facilities of the department for compliance with POPIA

15.3.6. Annually review the electronic transmission flows of personal information held by the Department and advise the Information Officer on the most feasible means of recording processing of personal information

15.3.7. Ensure the display of POPIA notices on the e-mail system

15.3.8. Ensure that reasonably necessary technical measures to prevent unauthorised access to the information technology equipment / system are maintained and that any breach of the system is detected immediately

15.3.9. Ensure adequate business continuity measures are in place to protect personal information stored electronically from unintended destruction or loss

15.3.10. Manage compliance by SITA of its obligations in respect of POPIA

15.4 Communications

15.4.1. Ensure the display of POPIA notices on the website, on social media and at events

16 DUTIES OF FINANCE

16.1 Supply Chain Management

16.1.1. Ensure the display of POPIA notices on bidding documentation

16.1.2. Ensure that POPIA notices are communicated to new and existing service providers / suppliers

16.1.3. On an annual basis validate existing personal information of service providers / suppliers

16.1.4. Ensure that the contracts for operators are managed in compliance with this policy

16.2 Internal Control

16.2.1. Exercise internal control functions in respect of POPIA compliance by the Department

17 DUTIES OF SECURITY SERVICES

17.1. Provide guidance and assistance to employees in the department in respect of ensuring that physical security measures are taken to safeguard personal information

17.2. Ensure that reasonably necessary physical security measures to prevent unauthorised access to record storage facilities are maintained and any breach detected immediately

17.3. Annually review the Security Policy of the department to ensure alignment with POPIA

17.4. Review building access registers to ensure that only essential personal information is collected

17.5. Continuously review the need for prior authorisation from the Regulator in respect of security vetting processes and advise the Information Officer accordingly

18 DUTIES OF LEGAL SERVICES

18.1. Ensure that POPIA notices are communicated to new and existing complainants

18.2. Ensure that POPIA notices are sent to any new and existing litigants

18.3. Ensure that contracts with operators are in accordance with POPIA

18.4. Provide guidance and advice to the Department in respect of POPIA compliance

19 DUTIES OF RISK MANAGER

19.1. On an annual basis facilitate the development of a POPIA risk management plan and monitor the implementation thereof on a quarterly basis.

20 DUTIES OF PROVINCIAL SECRETARIAT FOR POLICE

20.1 Provincial Directors

20.1.1. Ensure that POPIA notices are sent to any new and existing stakeholder representatives

20.1.2. On an annual basis validate existing personal information of stakeholder representatives

20.2 Regional Directors

20.2.1. Ensure that POPIA notices are sent to any new and existing stakeholder representatives

20.2.2. On an annual basis validate existing personal information of stakeholder representatives

20.2.3. Ensure fulfilment by the District Offices of their responsibilities in terms of this policy

20.3 District Offices

20.3.1. Ensure that POPIA notices are communicated to new and existing complainants

20.3.2. Ensure that POPIA notices are sent to any new and existing members of safety structures

20.3.3. On an annual basis –

a) validate existing personal information of volunteers;
b) validate existing personal information of District Office Employees;
c) validate existing personal information of complainants;
d) validate existing personal information of safety structures members.

21 POPIA COMMITTEE

21.1 Terms of Reference

21.1.1 <u>Functions</u>

The functions of the Committee are to –

a) oversee compliance by the department with POPIA;
b) review compliance policies, strategies, procedures, frameworks and programmes and the monitoring thereof and make recommendations thereon to the Information Officer;
c) consider reports on the fulfilment of the responsibilities contemplated in this policy;
d) review complaints relating to the processing of personal information by the Department and make recommendations thereon to the Information Officer;
e) review the impact assessments undertaken by the Department and make

recommendations to the Information Officer;

f) review the POPIA risk management plan and make recommendations thereon to the Risk Manager;
g) generally advise the Information Officer on matters affecting the protection of the personal information of data subjects processed by the Department.

21.1.2 Composition

a) The Committee is composed of the following members:
    i. Director: Integrated Planning, Monitoring & Evaluation
    ii. Director: Corporate Services;
    iii. Director: Security Services;
    iv. Chief Financial Officer;
    v. Risk Manager;
    vi. Director: Legal Services;
    vii. A Regional Director designated by the Provincial Secretary for Police from time-to-time.
b) In the event a Member is not able to attend a meeting, such member may designate another official in his or her directorate at the level of deputy director to attend a meeting on his or her behalf.

21.1.3 Meetings

Frequency of Meetings

a) The Committee must meet at least quarterly;
b) Special meetings may be convened in cases of emergency; or where the matter has to be dealt with by the Committee on an urgent basis and cannot stand over to the next meeting;
c) Reasonable notice of the Committee meetings must be given to all members of the Committee;
d) Meetings may be held in person or through electronic means such as e-mail, tele-conference or video conference;

Chairing of Meetings

e) The Chairperson of the Committee is the Director: Integrated Planning, Monitoring & Evaluation.
f) The Chairperson must convene and Chair the meetings.
g) If the Chairperson is unable to attend a meeting the members will appoint a Chairperson for that meeting.

Quorum

h) At least three members must be present in the meeting.
i) A Committee meeting may, however, proceed with its business irrespective of the number of members present, but may not take a decision on any matter when there is no quorum.

Decision-making

j) The decisions are taken by consensus. Dissenting views must be recorded.

21.1.4 Secretariat

a) The Office of the Chairperson must provide secretariat services to the Committee. Minutes of all Committee meetings must be kept by the duly appointed secretariat of the meeting.
b) Minutes of the meetings of the Committee must record in sufficient detail the matters considered by the Committee and decisions reached, including any concerns and views raised by members.
c) Draft and final versions of minutes of such meetings should be sent to members of the Committee for comment and record respectively.
d) Adopted minutes must be signed by the Chairperson of the Committee.

21.1.5 Review and Evaluation

The Committee members must annually review and evaluate the adequacy of its

Committee and recommend any proposed changes to the Members for approval.

22 POPIA PROCEDURES

22.1 Validation of Personal Information

1. Responsibility Managers must on an annual basis validate the personal information held by their directorates by advising data subjects of the information held and requesting validation thereof.
2. Responsibility Managers must keep record of validation requests and responses and amend the personal information if necessary.
3. Responsibility Managers must report to the Deputy Information Officer on validation exercises undertaken and the Deputy Information Officer must report to the POPIA Committee on reports received.

22.2 Access to Personal Information

1. Data subjects have a right to access their personal information held by the Department.
2. Requests for access to personal information must be made in the prescribed format and directed to the Deputy Information Officer within 48 hours for processing within 30 days of receipt of the request.

22.3 Amendment of Personal Information

1. Data subjects have a right to amend their personal information held by the Department.
2. Requests for the amendment of personal information must be made in the prescribed format and directed to the Deputy Information Officer within 48 hours for processing within 30 days of receipt of the request.

22.4 De-identification of Personal Information

1. Responsibility Managers must on an annual basis review the personal information held by their directorates for purposes of establishing which personal information

could be de-identified without negatively affecting the purpose of collection of the information.

2. Any such personal information identified must be brought under the attention of the data subjects and the Director: Corporate Services.
3. The Director: Corporate Services must, after 30 days during which the data subjects could object to the intended de-identification and after consultation with the Deputy Information Officer, take the necessary steps for the de-identification of the personal information.
4. De-identification of personal information must be in accordance with the Records Management Policy and Disposal Directives applicable to the Department.
5. The Director: Corporate Services must report to the POPIA Committee and the Information Officer on the de-identification of personal information.

22.5 Destruction of Personal Information

1. Responsibility Managers must on an annual basis review the personal information held by their directorates for purposes of establishing in respect of which personal information the purpose of collection of the information has been fulfilled.
2. Any such personal information identified must be brought under the attention of the data subjects and the Director: Corporate Services.
3. The Director: Corporate Services must, after 30 days during which the data subjects could object to the intended destruction and after consultation with the Deputy Information Officer, take the necessary steps for the destruction of the personal information.
4. Destruction of personal information must be in accordance with the Records Management Policy and Disposal Directives applicable to the Department.
5. The Director: Corporate Services must report to the POPIA Committee and the Information Officer on the destruction of personal information.

22.6 Breach of Security of Personal Information

1. Any breach or suspected breach of security of personal information must immediately be reported to the relevant Responsibility Manager, the Deputy Information Officer, Director: Corporate Services and Director: Security Services.

2. In the event that the breach is of a physical nature, the Director: Security Services must take all reasonable steps to contain the consequences of the breach, re-establish adequate security measures and liaise with relevant law enforcement agencies in respect of the tracing of suspects and recovery of any personal information removed.
3. In the event that the breach is of a technical nature, the Director: Corporate Services must take all reasonable steps to contain the consequences of the breach and re-establish adequate security measures. The Director: Security Services must liaise with relevant law enforcement agencies in respect of the tracing of suspects and recovery of any personal information removed.
4. The Deputy Information Officer must compile a report for the Information Officer to the Regulator on the breach and remedial measures taken and must manage the communication to the affected data subjects.
5. The Deputy Information Officer must report to the POPIA Committee on any breach, remedial measures and communication to data subjects.

22.7 Complaints handling procedure

1. Any complaint relating to the processing of personal information by the Department must be made in the prescribed format and submitted to the Deputy Information Officer.
2. After investigating the complaint, the Deputy Information Officer must table a report with the POPIA Committee, who must in turn consider same and make a recommendation thereon to the Information Officer.
3. The complaints management process must be finalised within 30 days.

23 POPIA TEMPLATES

23.1 Notices

Notice Type	Annexure
POPIA E-mail, Website and Social Media Privacy Notice	B
POPIA Notice at Building Entrances	C
POPIA Supply Chain Management Notice	D

POPIA Notice to Complainants in respect of poor police service delivery	E
POPIA Notice for Post Advertisements	F
POPIA Notice for Appointees	G
POPIA Notice to Members of Safety Structures	H

23.2 Forms

POPIA Complaint Form – Annexure I
POPIA Request for Amendment of Personal Information Form – Annexure J

23.3 Registers

POPIA Personal Information Inventory – Annexure K

24 PERSONAL INFORMATION IMPACT ASSESSMENT

a) The Deputy Information Officer must facilitate a Personal Information Impact Assessment on an annual basis and table the outcome of the assessment with the POPIA Committee for consideration and recommendations thereon to the Information Officer.
b) The assessment must include an evaluation of the adequacy of the measures put in place to ensure the protection of personal information by the department.

25 APPROVAL OF THE POLICY

The Head of Department approves the Policy and all Districts and Units of the Department must comply with the Policy.

26 MONITORING OF THE POLICY

All Responsibility Managers must report to the Deputy Information Officer(s) on a quarterly basis on measures taken to implement the Police for review by the POPIA Committee.

27 REVIEW OF THE POLICY

The policy will be reviewed on an annual basis.

28 COMMENCEMENT

This policy commences on approval by the Head of Department.

29 SCOPE AND APPLICATION

This policy applies to officials of the department, its offices and units.

DCSL PROTECTION OF PERSONAL INFORMATION COMPLIANCE POLICY FRAMEWORK APPROVED BY INFORMATION OFFICER / HEAD OF DEPARTMENT ON THIS …… DAY OF …….. 2021

_____

MR BS GUMBI

INFORMATION OFFICER / HEAD OF DEPARTMENT

KWAZULU-NATAL PROVINCE
COMMUNITY SAFETY AND LIAISON
REPUBLIC OF SOUTH AFRICA

ANNEXURE A - MATRIX OF PERSONAL INFORMATION PROCESSED BY DEPARTMENT

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
Human Resources	Applicants for employment	Names, IDs, addresses, contact details, race, gender, experience, qualifications, employment details	To process applications for employment	Direct	Receive, screening, verification, evaluate during recruitment process and filing	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(d) S29**
	Employees and dependents	Names, IDs, PERSAL numbers, addresses, contact details, race, gender, experience, qualifications, employment details	To process career incidents	Direct & indirect	Appointment processes, PERSAL administration, leave administration, performance management, discipline management, medical aid and pension form processing, resignation / retirement processing	Physical files and electronic (hard drives, server, transversal system)	Records Management Policy	**S11(1)(d) S12(2)(c) S32(f)(i) Note: S30 only authorizes Trade Union to process information on union affiliation, not employers;**
Fleet Management	Employee drivers of	Names, contact details	To process access to State vehicles	Direct	Issuing of trip authorities, processing of	Physical files and electronic	Records Management Policy	**S11(1)(d)**

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
	vehicles and passengers				application for subsidized vehicles	(hard drives, server)		
Information Technology	Employee users of system	Names, PERSAL number, e-mail addresses, passwords	To process access to IT system	Direct	Administration of access to system	Physical files and electronic (hard drives, server)	Records Management Policy	**S11(1)(d)**
Security Services	Visitors	Names, IDs, contact details	To process access to offices	Direct	Registration of access	Physical files	Records Management Policy	**S11(1)(a)**
	Employees	Names, IDs, PERSAL numbers, addresses, contact details, fingerprints	To process criminal records checks / vetting	Direct	Criminal record screening, security clearance processing	Physical files and electronic (hard drives, server)	Records Management Policy	**S11(1)(d)**
Asset Management	Employee users of assets	Names, PERSAL numbers	Process asset utilization and accountability	Direct	Recording of custodians of assets, reporting of losses	Physical files and electronic (hard drives, server, transversal system)	Records Management Policy	**S11(1)(d)**
Supply Chain Management	Bidders	Names, IDs, addresses, registration	To process the evaluation and award of bids	Direct	Processing quotations or bids	Physical files, electronic	Records Management Policy	**S11(1)(d)**

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
		numbers, contact details			(screening, verification, evaluation and filing)	(hard drives, server)		
	Contracted service providers	Names, IDs, addresses, registration numbers, contact details, bank account details	Contract management	Direct	Processing contracts through to Legal Services and end-users	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(b)**
Accounting Services	Employees	Names, IDs, PERSAL numbers, bank account details	To process claims and payments	Direct	Payroll management; subsistence and transport claim administration	Physical files and electronic (hard drives, server, transversal system)	Records Management Policy	**S11(1)(d)**
	Service providers and creditors	Names, IDs, addresses, registration numbers, contact details, bank account details	To process claims, invoices and payments	Direct	Capturing banking details, processing payments	Physical files and electronic (hard drives, server, transversal system)	Records Management Policy	**S11(1)(b)**

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
Legal Services	Contracted service providers	Names, IDs, addresses, registration numbers, contact details, bank account details	To process the drafting and signing of contracts	Indirect	Receiving bids / quotations, drafting contracts	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(b) S12(2)(c)**
	Litigants and claimants	Names, IDs, addresses, registration numbers, contact details, bank account details	Administering court processes, claims, correspondence	Indirect	Filing claims, correspondenc, transmitting documentation to attorneys	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(d) S12(2)(d)(iii)**
	Employees	Names, contact details	Assessing liability for losses	Direct	Filing requests and supporting docs, formulating opinions, transmitting same to CFO	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(d)**
	Complainants	Names, IDs, addresses, registration numbers, CAS numbers,	Providing legal opinions on cases	Direct / Indirect	Filing requests and supporting docs, formulating opinions, transmitting	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(c), (d) & (e) S12(2)(c)**

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
		contact details			same to management			
Provincial Secretariat for Police	Complainants	Names, IDs, addresses, registration numbers, contact details	Investigation of complaints against police	Direct	Filing requests and supporting docs, transmitting same to SAPS, drafting reports to management, communicating with complainants	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(c), (d) & (e)**
	Parties in conflict	Names, IDs, addresses, registration numbers, contact details	Facilitating mediation processes	Direct	Filing supporting docs, transmitting same to SAPS and other stakeholders, drafting reports to management, communicating with parties	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(d)**
	Members of community safety structures	Names, IDs, addresses, registration numbers,	Facilitating the functionality of safety structures	Direct	Recording information, communicating information to other	Physical files, electronic (hard	Records Management Policy	**S11(1)(c), (d) & (e)**

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
		contact details			members, stakeholders and SAPS, sending communication to data subject regarding activities	drives, server)		
	Complainants / suspects / victims in criminal investigations	Names, IDs, addresses, registration numbers, contact details, CAS numbers	To assess the effectiveness of criminal investigations	Direct / Indirect	Filing requests and supporting docs, transmit same to SAPS / NPA, access dockets for review, drafting reports, transmitting same to management, communicating with complainants	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(c), (d) & (e) S12(2)(a) or (c)**
	Members of the public attending events / functions / workshops	Names, IDs, contact details	To facilitate participation in crime prevention programmes	Direct	Recording information in attendance registers, filing registers, making registers	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(c) / (e)**

Processing Component	Data Subjects	Personal Information	Processing Purpose	Collection	Processes	Record formats	Disposal of records	Authority for Processing
					available for auditing			
IGR and Special Projects	Volunteers	Names, IDs, PERSAL numbers, addresses, race, gender, bank account details	Processing applications, appointments, payments, discharge	Direct	Receiving / filing applications, conduct interviews, capture details on PERSAL and other systems, receiving / filing time-sheets, compile reports, submit details to DPW for EPWP administration	Physical files, electronic (hard drives, server)	Records Management Policy	**S11(1)(d) / (e)**

ANNEXURE B - DEPARTMENT OF COMMUNITY SAFETY & LIAISON (DCSL) PRIVACY NOTICE AND INFORMED CONSENT NOTICE

CONSENT TO PROCESS PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF INFORMATION ACT, 4 OF 2013 (POPIA) (EMAIL, WEBSITE AND SOCIAL MEDIA PRIVACY NOTICE)

The Protection of Personal Information Act, 4 of 2013 (POPIA), gives effect to the constitutional right to data privacy in terms of Section 14 of the Bill of Rights of the Constitution.

The responsible use of the DCSL website and related resources in respect of data privacy is important to DCSL.

Whilst DCSL is committed to protecting all person's rights to privacy and who in consequence will ensure that all person's Personal Information is used appropriately, transparently and according to applicable law, the DCSL has to ensure that these rights to privacy are balanced with other rights such as the right to use and have access to the DCSL Information and Services including its online and social media platforms and applications.

This Policy sets out the responsibilities and obligations of all persons who make use of, or access or receive DCSL Information and Communications via its electronic communication facilities and resources including its website, email and social media platforms and how all users of these facilities and resources are to ensure that when using these resources that they respect and process another's Personal Information lawfully and in accordance with the provisions of POPIA and the 8 Personal Information Processing Principles.

PLEASE READ THE DOCUMENT BEFORE YOU MAKE USE OF THE DCSL ELECTRONIC FACILITIES OR PROVIDE DCSL WITH ANY PERSONAL INFORMATION. BY PROVIDING DCSL WITH YOUR PERSONAL INFORMATION, YOU CONSENT TO THE DCSL PROCESSING YOUR PERSONAL INFORMATION, WHICH DCSL UNDERTAKES TO PROCESS STRICTLY IN ACCORDANCE WITH THIS PRIVACY POLICY.

INDEX TO POLICY

1. INTRODUCTION

1.1 DCSL in order to carry out its aims and objectives as Provincial Government Department responsible for police oversight and community safety initiatives will, on an ongoing basis receive, provide and process Personal Information.

1.2 In terms of the Protection of Personal Information Act, 4 of 2013 (POPIA) everyone has the right to privacy, including the right to the lawful collection, retention, dissemination and use of one's Personal Information.

1.3 In order to give effect to this right, DCSL is under a duty to provide any person whose Personal Information is processed by it, (known as a "Data Subject") with a number of details pertaining to the use of and subsequent processing of the Data Subject's Personal Information, before such Personal Information may be used or processed by DCSL.

1.4 In accordance with this requirement, DCSL sets out below:

- the reasons why it will have to process a Data Subject's Personal Information,
- the conditions under which it will receive and use a Data Subjects Personal Information,
- how DCSL will use and handle this Personal Information, as well as
- the conditions under which it will provide its own Personal Information.

2. APPLICATION

2.1 The Privacy Policy of DCSL, is applicable to –

2.1.1 all DCSL electronic platforms and facilities, including social media, websites and / or email, whether owned by, established by, used by, hosted by and / or accessed by DCSL;

2.1.2 all and any Data Subject(s), who may access and make use of the aforementioned DCSL electronic platforms and facilities, including, without detracting from the generality thereof, DCSL employees and staff, consumers and customers, vendors, contractors, service providers and / or other third parties;

2.2.2 all the Personal Information which is owned by DCSL and which is provided to any responsible parties and / or operators as a result of such person accessing or making use of the DCSL social media and electronic platforms.

3. ACCOUNTABILITY

3.1 DCSL takes the privacy and protection of a Data Subject's Personal Information very seriously and will only process a Data Subject's Personal Information in accordance with POPIA and the terms of this Privacy Policy.

3.2 In turn where DCSL provides any of its Personal Information to a Responsible Party or Operator, then such person will be required as a condition of receiving such information, to process such Personal Information in accordance with POPIA and the terms of this Privacy Policy.

3.3 Accordingly, the relevant data privacy principles relating to the processing of Personal Information, whether that belonging to DCSL or that belonging to a data subject (including, but not limited to, the collection, handling, transfer, sharing, correction, storage, archiving and deletion) will apply without exception, save where POPIA provides for such an exception, to all and any Personal Information provided by DCSL to another or received by DCSL as a result of the use of the DCSL electronic platforms and facilities.

4. AGREEMENT TO BE BOUND AND CONSENT TO PROCESS

4.1 By accessing or using the DCSL electronic platforms and facilities including all website and URL's,

any sites housed under its domain names and / or social media platforms, and / or when sending or receiving emails using the DCSL email, the Data Subject:

4.1.1 acknowledges that it has read and understood this Privacy Policy and related provisions;
4.1.2 agrees to be bound by this Privacy Policy;
4.1.3 agrees to comply with this Privacy Policy; and
4.1.4 gives DCSL consent to process and further process the required Personal Information for the required purpose, in accordance with this Privacy Policy.

5. RECEIPT, USE AND SHARING OF PERSONAL INFORMATION BY THE DCSL

5.1 DCSL will receive Personal Information pertaining to a Data Subject when the Data Subject submits a query or request via the DCSL electronic platforms or facilities, including via its website, or by way of email, telephone or via social media.

5.2 On receipt of the request or query, DCSL will thereafter use and process the Data Subject's Personal Information for the purpose of the query and for a variety of related purposes, which will all depend on the query or request, and which without detracting from the generality thereof may include:

- for the purposes of identifying and / or verifying the Data Subject's details;
- for the purposes of providing information and / or services or details in connection therewith or pertaining thereto, that the Data Subject, may have requested;
- human resource management relating to applicants for employment and employees;
- recruitment, deployment and payroll management of crime prevention volunteers;
- financial and supply chain management relating to suppliers, service providers and assets;
- security management;
- information technology management;
- monitoring and evaluation of police service delivery;
- investigation of complaints of poor police service delivery;
- promoting community police partnerships through support provided to community safety structures;
- facilitating the resolution of inter- and intra-community conflicts;
- undertaking community safety related research;
- community engagement on community safety related issues;
- internal planning, monitoring and evaluation of performance of the DCSL.

5.3 In order to correctly handle any request or query, and in order to perform the purposes described above, DCSL may from time to time share a Data Subject's Personal Information with the following parties:

- DCSL employees, which will only be done on a need to know basis;
- DCSL suppliers, which will only be done on a need to know basis;
- DCSL carefully selected stakeholders who provide services which may be of benefit to a Data Subject which will only be done on a need to know basis; and
- DCSL operators such as service providers and agents who perform services on behalf of the DCSL which will only be done on a need to know basis and in terms of a DCSL operator agreement.

5.4 DCSL does not share a Data Subject's Personal Information with any third parties who have not been described above, unless:

- DCSL is legally obliged to provide such information to another for legal or regulatory purposes;
- DCSL is required to do so for purposes of existing or future legal proceedings;
- the onward transmission or sharing of Personal Information is necessary for the pursuance or protection of DCSL legitimate interests or that of the Data Subject or a third party;
- DCSL are involved in the prevention of fraud, loss, bribery or corruption and are using another agent or service provider under a mandate to provide such service, and the agent or service provider needs to process the Data Subject's Personal Information for the purpose of investigating and or preventing any act of fraud, loss, bribery or corruption,

and under all of the abovementioned circumstances, DCSL will take reasonable measures to ensure that such Personal Information is only provided to the recipient, if such recipient undertakes to keep the Personal Information confidential and secure.

5.5 Where DCSL has to transfer the Data Subject's Personal Information across the South African borders, it will before it does so, ensure that the recipient thereof agrees to be bound by POPIA under and in terms of a set of binding corporate rules or binding agreements that provide an adequate level of protection and uphold the principles for the reasonable and lawful processing of such Personal Information.

6. RECEIPT, USE AND SHARING OF THE DCSL PERSONAL INFORMATION

DCSL on receipt and in response to a query or request received from a Data Subject, referred to under section 5 above, may transmit via its website, or by way of email, telephone or via social media, its own Personal Information, which Personal Information on receipt by the requesting or receiving party, may only be used for the purpose relating to the initiating of the request or query and for no other purpose.

Furthermore, the recipient undertakes that it will not use this Personal Information for any other purpose or share this information with any other party, save where it has been given express permission to do so by DCSL.

7. INFORMATION QUALITY/OPENNESS/DATA SUBJECT PARTICIPATION

7.1 Whilst DCSL will make all effort to ensure the integrity and accuracy of a Data Subject's Personal Information, this may not at all times be possible. Following this, the Data Subject accepts the responsibility for keeping his / her or its Personal Information up to date, and undertakes to inform DCSL of anychanges to his / her and its Personal Information.

7.2 A Data Subject has a right of access to any Personal Information which DCSL may have and where applicable may ask DCSL to correct any inaccuracies in or to any such Personal Information. Any access request must be done by way of a formal **DCSL PAIA process**, which is accessible on www.kzncomsafety.gov.za

8. SECURITY OF PERSONAL DATA

8.1 DCSL makes all reasonable effort to keep its social media and electronic platforms including its website secure at all times, however the DCSL advises that it cannot guarantee the security of any information provided to the DCSL or by the DCSL through the DCSL website, e-mail, internet or social media sites. Following this the DCSL cannot be held responsible for any loss or unauthorised use or interception of information transmitted via these social media and electronic platforms or sites, including its Internet, which is beyond the DCSL reasonable control.

8.2 The DCSL website may contain links to other websites outside of DCSL control. DCSL is not responsible for the content, privacy or security of these other third party controlled websites.

8.3 DCSL has placed cookies on its website which makes contact with your / a Data Subject's device to help make the DCSL social media and electronic platforms website better.

8.4 DCSL makes use of social plugins of social networks such as Facebook, YouTube, LinkedIn, Google+ and Twitter. Please note that DCSL has no influence on or control over the extent of the data retrieved by the social networks' interfaces and DCSL can accordingly not be held responsible or liable for any processing or use of Personal Information transmitted via these social plugins. For information on purpose and extent of the data retrieval by the social network concerned, and about the rights and settings which are available for you to access for the protection of your private information, please refer to the data protection information provided by the social network in question.

8.5 Note that all DCSL social media and electronic platforms including its website and telephone facilities and your use of them will be monitored on a regular basis including the recordal and interception of content placed on or stored on said facilities which is done for security, integrity and quality assessment purposes and by using such electronic platforms and facilities you expressly acknowledge notice of such monitoring and interception and give consent thereto in accordance with the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 ("RICA"),

8.6 Subject to the provisions above, DCSL has implemented the appropriate technical and organisational security measures which are required in order to protect all Personal Information and related data which it holds from and / or against unauthorised access, accidental or willful manipulation, loss or destruction.

9. THIRD PARTY INFORMATION AND THAT BELONGING TO MINORS

9.1 If a Data Subject provides DCSL with Personal Information on behalf of another, DCSL will not be able to process the query or request unless such query or request is accompanied with the required permission and consent from the owner of that Personal Information.

9.2 If a Data Subject is under the age of 18, such person's Personal Information will only be processed if the minor's parent or legal guardian gives the required consent or permission to the processing of the provided Personal Information.

10. CONTACT DETAILS

You can contact DCSL in relation to this Privacy Policy by writing to us at info@comsafety.gov.za or by calling our Head Office on 033-3419300.

11. REVISION OF POLICIES

DCSL reserves the right to and may from time to time update this Privacy Notice. Any such revision will be published as an amended version on the DCSL website.

Following this, any change to this Policy will be posted as an updated version and readers are advised to visit and re-read this policy on a regular basis.

ANNEXURE C - BUILDING ACCESS SECURITY NOTICE

Entry upon these premises is subject to the Control of Access to Public Premises and Vehicles Act, 1985 (Act No. 53 of 1985), and any person entering these premises are, in terms of section 2(2) of this Act, required to furnish his/her name, address and any other relevant information required by the security officer and produce proof of his/her identity to the satisfaction of the security officer. Provision of this personal information is mandatory in order to gain entry to the premises and failure to provide same would result in entry being refused.

The Department of Community Safety and Liaison (hereafter 'the department') and/or its security service provider collects and processes the personal information so provided for purposes of security management of the premises, including, but not limited to taking appropriate action in the event of any security breach or incident. The personal information may also be disclosed when –

- the department has a duty or a right to disclose same in terms of any law; or
- it is necessary to protect the rights of the department.

The information will be retained for a period of …….. before it is archived/destroyed.

Any person entering these premises thereby consents to the processing of personal information in accordance with the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), and acknowledge his/her right to –

- access and rectify the information collected;
- object to the processing of personal information to protect a legitimate interest or processing that is necessary for the proper performance of a public law duty by a public body, on reasonable grounds relating to his/her particular situation, unless legislation provides for such processing; and
- lodge a complaint to the Regulator at complaints.IR@justice.gov.za.

ANNEXURE D - SUPPLY CHAIN MANAGEMENT NOTICE

PROTECTION OF PERSONAL INFORMATION ACT, 2013
DECLARATION BY PROSPECTIVE SUPPLIERS / SERVICE PROVIDERS

The Department of Community Safety and Liaison (hereafter 'the department') and its employees collect and process the personal information of prospective suppliers or service providers for purposes of supply chain management, including, but not limited to, –

1. *evaluating and adjudicating quotations or bids;*
2. *communication with suppliers or service providers;*
3. *drafting contracts such as Service Level Agreements;*
4. *contract management;*
5. *taking appropriate action in the event of any breach of contract;*
6. *payment of invoices; and*
7. *compiling reports.*

The personal information may also be disclosed or processed when –

- *the department has a duty or a right to disclose same in terms of any law; or*
- *it is necessary to protect the rights of the department.*

I declare that all the information provided (including any attachments) is complete and correct to the best of my knowledge. I understand that -

i. *the supply of this information is mandatory in order to evaluate the quotation or bid in pursuance of the request for quotation or tender;*
ii. *failure to supply same would result in disqualification; and*
iii. *any false information may result in criminal prosecution and/or being reported to Treasury.*

The personal information collected may be shared with and processed by –

1. *the BAS system and administrators of the system;*
2. *the Provincial and National Treasury;*
3. *the State Information Technology Agency;*
4. *the Auditor-General;*
5. *Law enforcement agencies;*
6. *the South African Revenue Services;*
7. *Provincial Archives; or*
8. *any other Organs of State for purposes of performing their public functions or their agents.*

I acknowledge that any personal information shall be retained for a period of …. years before being destroyed by the Provincial Archives. I accept that the processing of the personal information shall be in accordance with the Protection of Personal Information Act, 2013 and shall be for any one or more of the following purposes:

a) *processing necessary for supply chain management;*

b) *processing in pursuance of an obligation imposed by law on the Public Service;*
c) *processing in order to protect a legitimate interest of mine / the company;*
d) *processing necessary for the proper performance of a public law duty of the Public Service; or*
e) *processing necessary for pursuing the legitimate interests of the Public Service or of a third party to whom the information is supplied.*

I hereby consent to the processing of personal information in accordance with the Protection of Personal Information Act, 2013 and I acknowledge that I have the right to –

i. *access to and the right to rectify the information collected;*
ii. *the right to object to the processing of personal information to protect a legitimate interest or processing that is necessary for the proper performance of a public law duty by a public body, on reasonable grounds relating to my particular situation, unless legislation provides for such processing; and*
iii. *lodge a complaint to the Regulator (complaints.IR@justice.gov.za).*

SIGNATURE (DULY AUTHORISED) **DATE**

FULL NAMES: ……..

COMPANY NAME: ……

ANNEXURE E - NOTICE TO POLICE SERVICE DELIVERY COMPLAINANTS

PROTECTION OF PERSONAL INFORMATION ACT, 2013

NOTICE & DECLARATION BY COMPLAINANT IN RESPECT OF POOR POLICE SERVICE DELIVERY

The Department of Community Safety and Liaison (hereafter 'the department') and its employees collect and process the personal information of complainants in respect poor police service delivery for purposes of complaints management, including, but not limited to, –

1. *investigating complaints;*
2. *communication with the police and other relevant stakeholders;*
3. *compiling reports; and*
4. *giving feedback to complainants.*

The personal information may also be disclosed or processed when –

- *the department has a duty or a right to disclose same in terms of any law; or*
- *it is necessary to protect the rights of the department.*

If a Data Subject provides DCSL with Personal Information on behalf of another, DCSL will not be able to process the query or request unless such query or request is accompanied with the required permission and consent from the owner of that Personal Information.

If a Data Subject is under the age of 18, such person's Personal Information will only be processed if the minor's parent or legal guardian gives the required consent or permission to the processing of the provided Personal Information.

I declare that all the information provided (including any attachments) is complete and correct to the best of my knowledge. I understand that -

i. *the supply of this information is mandatory in order to have the complaint investigated;*
ii. *failure to supply same would result in my complaint not being investigated; and*
iii. *any false information may result in criminal prosecution and/or being reported to Treasury.*

The personal information collected may be shared with and processed by –

1. *employees of the Department;*
2. *the South African Police Service / Metro Police Service;*
3. *other relevant stakeholders in the Criminal Justice System;*
4. *the State Information Technology Agency;*
5. *the Auditor-General;*
6. *Provincial Archives; or*
7. *any other Organs of State for purposes of performing their public functions or their agents.*

I acknowledge that any personal information shall be retained for a period of …. years before being destroyed by the Provincial Archives. I accept that the processing of the personal information shall be in accordance with the Protection of Personal Information Act, 2013 and shall be for any one or more of the following purposes:

a) *processing necessary for complaints management;*
b) *processing in pursuance of an obligation imposed by law on the Public Service;*
c) *processing in order to protect a legitimate interest of mine / the organisation I represent;*
d) *processing necessary for the proper performance of a public law duty of the Public Service; or*
e) *processing necessary for pursuing the legitimate interests of the Public Service or of a third party to whom the information is supplied.*

I hereby consent to the processing of personal information in accordance with the Protection of Personal Information Act, 2013 and I acknowledge that I have the right to –

i. *access to and the right to rectify the information collected;*
ii. *the right to object to the processing of personal information to protect a legitimate interest or processing that is necessary for the proper performance of a public law duty by a public body, on reasonable grounds relating to my particular situation, unless legislation provides for such processing; and*
iii. *lodge a complaint to the Regulator (complaints.IR@justice.gov.za).*

SIGNATURE (DULY AUTHORISED) **DATE**

FULL NAMES: …….

COMPANY NAME: ……

ANNEXURE F - NOTICE FOR POST ADVERTISEMENTS

PROTECTION OF PERSONAL INFORMATION ACT, 2013
NOTICE & DECLARATION BY APPLICANTS FOR EMPLOYMENT

I declare that all the information provided (including any attachments) is complete and correct to the best of my knowledge. I understand that

i. *the supply of this information is mandatory in order to process the application for employment and to comply with the laws regulating employment matters in the Public Service;*
ii. *failure to supply same would result in disqualification;*
iii. *any false information provided will result in criminal action being taken that may result in my prosecution.*

The personal information collected through the application may be shared with and processed by –

1. *the employees of the Department for purposes of administering the recruitment and selection process;*
2. *employees of other Departments and entities serving on selection / interview panels;*
3. *Law enforcement agencies for purposes of criminal record checks;*
4. *Third parties contracted by the Department to undertake any vetting process in relation to the application; and*
5. *any other Organs of State for purposes of performing their public functions or their agents.*

I acknowledge that any personal information shall be retained for …. years before being destroyed. I accept that the processing of the personal information shall be in accordance with the Protection of Personal Information Act, 2013 and shall be for any one or more of the following purposes:

a) *processing necessary to manage my application for employment within the Public Service in accordance with the laws applicable to the Public Service;*
b) *processing in pursuance of an obligation imposed by law on the Public Service;*
c) *processing in order to protect a legitimate interest of mine;*
d) *processing necessary for the proper performance of a public law duty of the Public Service; or*
e) *processing necessary for pursuing the legitimate interests of the Public Service or of a third party to whom the information is supplied.*

I hereby consent to the processing of personal information in accordance with the Protection of Personal Information Act, 2013 and I acknowledge that I have the right to –

i. *access to and the right to rectify the information collected;*
ii. *the right to object to the processing of personal information to protect a legitimate interest or processing that is necessary for the proper performance of a public law duty by a public body, on reasonable grounds relating to my particular situation, unless legislation provides for such processing; and*

iii. lodge a complaint to the Regulator (complaints.IR@justice.gov.za).

SIGNATURE **DATE**

ANNEXURE G - NOTICE TO APPOINTEES

PROTECTION OF PERSONAL INFORMATION ACT, 2013
NOTICE & DECLARATION BY APPOINTEES

I declare that all the information provided (including any attachments) is complete and correct to the best of my knowledge. I understand that -

i. *the supply of this information is mandatory in order to process the appointment / transfer and to comply with the laws regulating employment matters in the Public Service;*
ii. *failure to supply same would result in non-appointment / transfer;*
iii. *any false information provided will result in disciplinary action being taken that may result in my dismissal.*

The personal information collected may be shared with and processed by –

1. *the PERSAL system and administrators of the system;*
2. *the State Information Technology Agency;*
3. *the Auditor-General;*
4. *Law enforcement agencies;*
5. *the South African Revenue Services;*
6. *the Government Employees Pension Fund;*
7. *the Government Employees Medical Aid Scheme; and*
8. *any other Organs of State for purposes of performing their public functions or their agents.*

I acknowledges that any personal information shall be retained for the duration of my employment in the Public Service and for an additional period of …. years after my resignation / retirement / death before being destroyed. I accept that the processing of the personal information shall be in accordance with the Protection of Personal Information Act, 2013 and shall be for any one or more of the following purposes:

a) *processing necessary to manage my employment within the Public Service in accordance with the laws applicable to the Public Service;*
b) *processing in pursuance of an obligation imposed by law on the Public Service;*
c) *processing in order to protect a legitimate interest of mine;*
d) *processing necessary for the proper performance of a public law duty of the Public Service; or*
e) *processing necessary for pursuing the legitimate interests of the Public Service or of a third party to whom the information is supplied.*

I hereby consent to the processing of personal information in accordance with the Protection of Personal Information Act, 2013 and I acknowledge that I have the right to –

i. *access to and the right to rectify the information collected;*
ii. *the right to object to the processing of personal information to protect a legitimate interest or processing that is necessary for the proper performance of a public law duty by a public body, on reasonable grounds relating to my particular situation, unless legislation provides for such processing; and*

iii. lodge a complaint to the Regulator (complaints.IR@justice.gov.za).

SIGNATURE **DATE**

ANNEXURE H - NOTICE TO MEMBERS OF COMMUNITY SAFETY STRUCTURES

PROTECTION OF PERSONAL INFORMATION ACT, 2013

NOTICE TO MEMBERS OF COMMUNITY SAFETY STRUCTURES

The Department of Community Safety and Liaison (hereafter 'the department') and its employees collect and process the personal information of community safety structures in order to fulfil its Constitutional mandate of promoting good relations between the police and communities, including, but not limited to, –

1. *providing logistical and administrative support to community safety structures;*
2. *assessing the functionality of community safety structures;*
3. *investigating complaints of poor community police relations;*
4. *communication with the police and other relevant stakeholders in respect of community police relations;*
5. *compiling reports; and*
6. *giving feedback to communities.*

The personal information may also be disclosed or processed when –

- *the department has a duty or a right to disclose same in terms of any law; or*
- *it is necessary to protect the rights of the department.*

If a Data Subject provides DCSL with Personal Information on behalf of another, DCSL will not be able to process the query or request unless such query or request is accompanied with the required permission and consent from the owner of that Personal Information.

If a Data Subject is under the age of 18, such person's Personal Information will only be processed if the minor's parent or legal guardian gives the required consent or permission to the processing of the provided Personal Information.

The personal information collected may be shared with and processed by –

1. *employees of the Department;*
2. *the South African Police Service / Metro Police Service;*
3. *other relevant stakeholders in the Criminal Justice System;*
4. *the State Information Technology Agency;*
5. *the Auditor-General;*
6. *Provincial Archives; or*
7. *any other Organs of State for purposes of performing their public functions or their agents.*

By providing the personal information to the Department, the Data Subject acknowledges that any personal information shall be retained for a period of …. years before being destroyed and that the processing of the personal information shall be in accordance with the Protection of Personal Information Act, 2013 and shall be for any one or more of the following purposes:

a) *processing necessary for promoting good community police relations or crime prevention;*
b) *processing in pursuance of an obligation imposed by law on the Public Service;*
c) *processing in order to protect a legitimate interest of the Data Subject / the organisation represented by the Data Subject;*
d) *processing necessary for the proper performance of a public law duty of the Public Service; or*
e) *processing necessary for pursuing the legitimate interests of the Public Service or of a third party to whom the information is supplied.*

By providing the personal information to the Department, the Data Subject consents to the processing of personal information in accordance with the Protection of Personal Information Act, 2013 and acknowledges the right to –

i. *access to and the right to rectify the information collected;*
ii. *the right to object to the processing of personal information to protect a legitimate interest or processing that is necessary for the proper performance of a public law duty by a public body, on reasonable grounds relating to my particular situation, unless legislation provides for such processing; and*
iii. *lodge a complaint to the Regulator (complaints.IR@justice.gov.za).*

ANNEXURE I - POPIA COMPLAINT FORM

KZN DCSL

Objection / Complaint to the processing of Personal Information

Note: Affidavits or other documentary evidence as applicable in support of the objection may be attached.

Hard copy objections / complaints can be submitted to:

Postal Address: The Deputy Information Officer Private Bag X9143, Pietermaritzburg, 3200	**Physical Address:** The Deputy Information Officer 179 Jabu Ndlovu Street, Pietermaritzburg, 3201

By E-mail: info@comsafety.gov.za

Details of Complainant / Data Subject:

First Name: _____

Last Name: _____

Address: _____

Contact: _____

Fax Number / Email: _____

Reasons for Objection/Complaint:

_____

_____

_____

_____

_____

Signature Below:

_____

Date: _____

ANNEXURE J - POPIA REQUEST FOR AMENDMENT OF PERSONAL INFORMATION

KZN DCSL

Request for the Amendment of Personal Information

Note: Any documentary evidence as applicable in support of the request may be attached.

Hard copy requests can be submitted to:

Postal Address:	**Physical Address:**
The Deputy Information Officer Private Bag X9143, Pietermaritzburg, 3200	The Deputy Information Officer 179 Jabu Ndlovu Street, Pietermaritzburg, 3201

By E-mail: info@comsafety.gov.za

Details of Data Subject:

First Name: _____

Last Name: _____

Address: _____

Contact: _____

Fax Number / Email: _____

Details of Request to Amend Personal Information:

_____

_____

_____

_____

_____

Signature Below:

_____

Date: _____

KWAZULU-NATAL PROVINCE
COMMUNITY SAFETY AND LIAISON
REPUBLIC OF SOUTH AFRICA

ANNEXURE K - POPIA PERSONAL INFORMATION INVENTORY

Personal Information Medium	Data Subject (s)	Personal Information Capture Point(s)	Personal Info Content	Processing Transactions	Storage Medium	Storage Facility	Storage Location	Storage Custodian	Officials with Access	Access Protocols	Physical Security Measures	Logical Security Measures	Disposal Period	Disposal Method	Third Party Transfer
Example: Leave Form	Employees	Directorates / Units; Personnel Officers	Employee Name; PERSAL No; Address; Cellphone number	Receive leave forms; transmit to HRM; Capture information on PERSAL System; Retrieving for audit purposes	Hardcopy files	Safe	Room 211, 179 Jabu Ndlovu Street	Mark Ferreira, Cell: 0836858497	Vinod Partha p; Dawn Chalmers	Obtain key from custodian; Complete access register	Lockable safe; office locked	PERSAL Password changed every 30 days; User Declaration	5 years	Destruction	PERSAL Admin; Internal Audit; Auditor-General; Registry to Provincial Archives