a world class African city

CITY OF JOHANNESBURG MUNICIPALITY POLICY ON

PROTECTION OF PERSONAL INFORMATION (POPI ACT)

POLICY NUMBER	
VERSION	**Version 1**
APPROVING AUTHORITY	City Manager
APPROVAL DATE	Draft
PUBLICATION DATE	November 2022
POLICY CUSTODIAN	Office of City Manager – Data Governance and Information Management Section
APPLICABILITY OF POLICY	The policy applies to COJ Employees, Councillors and COJ residents

1. BACKGROUND

The Protection of Personal Information Act, Act No. 4 of 2013 (POPIA), which came into force from 1 July 2021, is the comprehensive data protection legislation enacted in South Africa. It is therefore compulsory for all businesses within the private and public sectors that process personal information in South Africa to comply. The Act seeks to protect and regulate the processing of personal information into the broader Constitutional right to privacy.

POPIA requires businesses within the private and public sectors to regulate how information is organised, stored, secured, and discarded. This ensures that the business can maintain the integrity and confidentiality of its clients' and employees' personal information by preventing loss, damage, and unauthorised access to the personal data. The Act therefore guarantees that personal information will be used in a responsible and ethical manner by businesses from the time it is collected until the time it is destroyed.

2. PURPOSE OF THE POLICY

The purpose of this policy is to give effect to the provision of POPIA to safeguard personal information of employees, potential consumers, consumers and third parties of COJ. In doing so, the City is committed to the observance of, and compliance with, the directives of the Constitution and national legislation alike, including the Protection of Personal Information Act. COJ endorses the key principles of good governance, transparency and accountability and seeks to regulate the use and Processing of Personal Information as lawfully required.

3. OBJECTIVES

The aim and objective of this policy is to:

3.1 ensure that personal information of COJ residents is adequately protected to avoid unauthorized access and use.

3.2 agree to protect personal information of COJ Councillors and employees. The personal information will be used appropriately, transparently, and securely in accordance with applicable laws.

3.3 to commit to protecting personal information of COJ residents, and employees.

4. DEFINITIONS

Below are the definitions relevant to this Guidance Note. For a complete list of definitions, please refer to the Protection of Personal Information Act 4 of 2013 (POPIA)

4.1 **"COJ"** means the City of Johannesburg Municipality;

4.2 **"The City** means the City of Johannesburg Municipality;

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

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

4.5 **''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

4.6 **"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

4.7 **"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, identity document/passport number, phone number, email address, financial information, physical address, date of birth, criminal record, private correspondence and online identifier or other particular assignment to the person;

b) Information relating to the educational or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; and

c) The name of the individual, where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

4.8 **"Public Body"** means any department or state administration in the national or provincial sphere of government or any municipality in the local sphere of government; or any other functionary or institution

when exercising a power or performing a duty in terms of the constitution or a provincial constitution or exercising a public power or performing a public function in terms of any legislation.

4.9 **"Processing"** means any operation or activity or any set of activities, whether or not by automatic means, concerning personal information including:

a) The collecting, receipting, recording, organizing, collation, storing, 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.

5. LAWFUL PROCESSING OF INFORMATION

POPIA sets out the following conditions for the lawful processing of personal information.

These conditions are not applicable to the processing of personal information to the extent that such processing is exempted in terms of section 37 or 38, from one or more of the conditions concerned in relation to such processing.

a) Duty by a public body.
b) Legal obligation to perform the processing of personal information.
c) Processing limitation – information may only be processed if it is adequate relevant and not excessive given the purpose for which it is collected.
d) Purpose specification – personal information must be collected for a specific, explicitly defined and lawful purpose related to the activity of the responsible party.
e) Further processing limitation – where information is received from a third party and passed on to the responsible party for further processing, the further processing must be compatible with the purpose for which it was initially processed.
f) Information quality – information must be complete, accurate, not misleading and updated where necessary.
g) Openness – the data subject must be informed when collecting information and the specific nature thereof.
h) Security safeguards - the responsible party must ensure the integrity of the personal information by taking measures to prevent the loss, damage or unauthorised destruction of the information.
i) Data subject specification – the data subject has the right to request a responsible person to confirm, free of charge, whether they hold personal information about them.

6. THE PERSONAL INFORMATION COLLECTED

6.1 In terms of section 9 of POPIA, personal information may only be processed if given the purpose for which it is processed, it is adequate, relevant and not excessive. Consequently, COJ collects personal information for the following reasons:

a) Registration of persons who apply and qualify for registration in COJ departments such as Revenue, Health, Licensing, Housing etc.

b) Personal information is collected for human resources and financial purposes, contractual relationships with third-party service providers who process personal data on behalf of COJ.

6.2 COJ collects personal information directly from data subjects. Examples of personal information collected from data subjects include but is not limited to:

- Applicant's name
- Registered professionals' names;
- Candidate's names;
- Categories of registration information;
- Status of registration;
- Foreign Applicants personal information
- Identity number;
- Date of birth;
- Gender;
- Race;
- Physical and Postal addresses;
- Employment details;
- Contact numbers;
- Email addresses;
- Academic information and records;
- Records of experience in the profession;

- Copies of qualifications;
- Curriculum Vitae; and
- Referee and mentor details.

6.3 COJ collects the following employees' personal information

- Name, address, phone number, cell numbers, marital status, date of birth;
- Next of kin;
- Doctor's name;
- spouse/partner contact information;
- Curriculum Vitae;
- Letters of reference;
- Employment status and history;
- Academic records;
- Banking details;
- Income tax reference number
- Disciplinary information;
- Salary information; and
- Criminal records.

6.4 COJ collects Council, Investigation Committees and Disciplinary Tribunal members' personal information:

- Surname
- First names
- Initials
- Marital Status
- Male/Female
- Date of Birth
- ID number

- Passport number
- Passport Country of issue
- Income tax reference number
- Address
- Banking details

6.5 COJ departments collect the following information from the public:

- Names, telephone numbers,
- Company from which a visitor comes from;
- Names of persons lodging complaints of improper conduct against other persons;
- Email addresses, identity number;
- Physical addresses;
- Email correspondence;
- Proof of payments;
- Personal information used on Service level agreements; and
- Service provider personal information

7. USE OF PERSONAL INFORMATION

7.1 Applicants, Customers, Service Providers, Visitors, Council and Committee members, and Employees' personal information will only be used for purposes for which it was collected and intended. This includes:

- Registration;
- Staff development
- Continuing Professional Development points;
- For audit and record keeping purposes;
- Investigations;
- Disciplinary processes;

- Nomination of Council members;
- Providing information on registered persons to SAQA (NRLD);
- Communicating with registered persons;
- Employee contracts;
- Communication with employees;
- Employee personal information is used to establish, manage, and terminate employment; and
- Analysis and review of service provider contracts, in terms of which personal information is processed for and on behalf of COJ.

7.2 According to section 10 of POPIA, personal information may only be processed if certain conditions are met, for instance:

- Consent is obtained to process personal information- in COJ's case consent obtained during registration, employment and entering into a service level agreement with service providers.
- Processing complies with an obligation imposed by law.

8. DISCLOSURE OF PERSONAL INFORMATION

a) COJ may disclose personal information where it has a duty or a right to disclose in terms of applicable laws.

b) COJ may disclose personal information where it deems necessary to protect the respect, dignity, and the professionalism of the Municipality.

c) COJ may disclose the Name and Surname of a registered person, his/her category of registration, registration number and the status of registration.

9. SAFEGUARDING REGISTERED PERSON'S PERSONAL INFORMATION

9.1 In terms of section 19 of POPIA, a responsible party must ensure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent: loss of, damage to or unauthorised destruction of personal information, unlawful access to or processing of personal information. POPIA requires that personal

information should be adequately protected to avoid unauthorised access. Therefore, COJ continuously reviews security controls and procedures to ensure that personal information is secured.

9.2 The following security controls are in place to protect personal information:

a) Personal information is treated as confidential and not disclosed unless required by law.

b) High level Information Technology controls are in place to maintain the protection of personal information.

c) High level anti-virus programs;

- Access rights in place;
- Computer passwords in place;
- Assessment of data quality controls in place to ensure the accuracy and completeness of personal information;
- A third-party service provider is mandated to ensure safeguarding of registered persons personal information;
- Personal information is stored at a third-party service provider who is subject to POPIA provision in the Service Level Agreement;
- COJ internal server hard drives are protected by firewalls;
- Employees, Council and Committee members of COJ sign confidentially agreements which is part of the employment contract;
- Hardcopy files are archived at a secured place.

10. ACCESS AND CORRECTION OF PERSONAL INFORMATION

a) Registered persons in COJ systems have a right to request for access to personal information in COJ's possession;

b) Registered persons' personal information should be continuously updated by information owners. This can be done electronically, telephonically by calling COJ departments or by calling COJ Call Centre.