



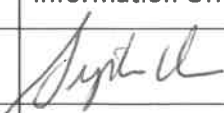
**NAME OF CLUSTER**  
**NAME OF THE POLICY**

<b>Policy Drafted or Review by</b>	
<b>Policy Implementing Departments</b>	
<b>Policy Mandated by</b>	
<b>Signature of Mandating Official</b>	<i>Siphiso Cele</i> Siphiso CELE Dem: Gov & IGR
<b>Approved by</b>	
<b>Date Adopted</b>	
<b>Date of Next Review</b>	
<b>Reviewed Yes/No</b>	



## GOVERNANCE AND INTERNATIONAL RELATIONS CLUSTER

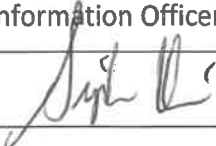
### PRIVACY POLICY

<b>Policy Drafted by</b>	POPI Steering Committee (PSC)		
<b>Document Change History</b>			
<b>Revision Date</b>	<b>Author</b>	<b>Revision No</b>	
October 2021	PSC	0	
Nov-Dec.21	PSC	1	
Jan-February 2022	PSC	2	
March 2022	PSC	3	
<b>Policy Implementing Departments</b>	All Departments		
<b>Policy Mandated by</b>	Information Officer. DCM Mr. Siphon Cele		
<b>Signature of Mandating Official</b>			
<b>Approved by</b>	Executive Management Committee		
<b>Date</b>	23/5/2022		
<b>Approved by</b>	EThekweni Municipality Council		
<b>Date</b>	30/6/2022		
<b>Date of Next Review</b>	May 2023		



## GOVERNANCE AND INTERNATIONAL RELATIONS CLUSTER

### PRIVACY POLICY

<b>Policy Drafted by</b>	POPI Steering Committee (PSC)	
<b>Document Change History</b>		
<b>Revision Date</b>	<b>Author</b>	<b>Revision No</b>
October 2021	PSC	New Policy
Nov-Dec.21	PSC	1
Jan-February 2022	PSC	2
March-April 2022	PSC	3
<b>Policy Implementing Departments</b>	All Departments	
<b>Policy Mandated by</b>	Information Officer. DCM Mr. Siphon Cele	
<b>Signature of Mandating Official</b>		
<b>Approved by</b>	Executive Management Committee	
<b>Date</b>	23 / 5 / 2022	
<b>Approved by</b>	EThekweni Municipality Council Exco	
<b>Date</b>	21 JUNE 2022	
<b>Date of Next Review</b>	May 2024	

## Table of Contents

1. GLOSSARY OF TERMS.....	3
2. LIST OF ABBREVIATIONS.....	7
3. Preamble .....	7
4. PURPOSE .....	7
5. SCOPE OF THE POLICY .....	8
6. OBJECTIVES OF THE POLICY .....	8
7. PRIVACY FRAMEWORK .....	8
8. INDEPENDENT REVIEW .....	8
9. LEGAL AND REGULATORY REQUIREMENTS.....	9
10. REFERENCE DOCUMENTATION.....	9
11. COMPLIANCE .....	9
12. ROLES AND RESPONSIBILITIES .....	10
12.1 POPI Information Officer.....	10
12.2 CISO.....	11
12.3 EThekwini Management .....	11
12.4 Employees, Contractors and Third Parties.....	11
13. POLICY STATEMENTS .....	11
13.1 Processing Limitation, Minimality and Consent.....	12
13.2 Purpose Specification and Retention .....	12
13.3 Further Processing Limitation .....	13
13.4 Information Quality and Data Subject Participation .....	13
13.5 Openness .....	13
13.6 Security Safeguards .....	14
13.7 Special Personal Information .....	14
13.8 Direct Marketing.....	15
13.9 Automated Decision-Making .....	15
13.10 International / Trans-border Information Flows .....	15
14. POLICY MONITORING AND EVALUATION AND POLICY REVIEW .....	16

## 1. GLOSSARY OF TERMS

Term	Definition
Best Practice	Recommendations or solutions that are considered the most desirable or preferred.
Biometric	A technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.
Consent	Any voluntary, specific, and informed expression of will in terms of which permission is given.
Control	A systematic measure implemented to minimise or mitigate risk.
Data	A set of values, numbers, characters, words, or other elements that may be interpreted or processed to produce information.
Data Subject	The person to whom personal information relates.
Direct Marketing	Approaching 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	Any text, voice, sound, image, or video message sent over an electronic network, such as e-mail, instant message (IM), SMS, WhatsApp, BBM message, unified communication, and video conferencing.
Employee	To this document, the term employee is considered to include all permanent, fixed term contracts and temporary individuals employed or appointed by the EThekweni Municipality.
Guideline	A document that provides recommended but not mandatory advice regarding practices in a given situation, scenario or topic.
Incident	An identified occurrence of an adverse event, indicating a possible breach of policy, failure of controls, or previously unknown situation that may have an impact on the information security and privacy responsibilities of an organisation.
Information Privacy	The right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination, and truthfulness of information about themselves.

Term	Definition
Information Processing Facility	Any information system, service, infrastructure, or the physical location that they are housed in.
Information Regulator	The public body formed under the POPI Act to regulate personal information handling practices in South Africa.
Information Resource	Any information in electronic, physical, or audio-visual form or any hardware, software or information processing facilities that makes possible the use, handling, transfer and/or storage of information.
Information Security Policy	A set of statements which express management's intent for the implementation, maintenance, and improvement of its information security.
Integrity	The property of information that describes its accuracy and completeness, especially as impacted by unauthorised modification.
Minimality	The use of only the smallest subset of information required to perform an activity or fulfil a duty
Must	An action/control that is mandatory
Person	A natural person or a juristic person

Term	Definition
Personal Information/Data	<p>Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—</p> <ul style="list-style-type: none"> <li>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;</li> <li>b) information relating to the education or the medical, financial, criminal or employment history of the person;</li> <li>c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;</li> <li>d) the biometric information of the person;</li> <li>e) the personal opinions, views or preferences of the person;</li> <li>f) correspondence sent by the person that is implicitly or explicitly of a private</li> <li>g) or confidential nature or further correspondence that would reveal the contents of the original correspondence;</li> <li>h) the views or opinions of another individual about the person; and</li> <li>i) 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</li> </ul>
Privacy Policy	<p>A formal document adopted by the EThekweni Municipality which express management's intent for the implementation, maintenance, and improvement of measures to protect information privacy. It governs an organisation's handling practices for personal information by specifying what can and cannot be done with the personal information.</p> <p>Complying with the policy is compulsory and failure and/or refusal to abide by it may be deemed as misconduct and may result in an investigation and/or disciplinary action against an employee.</p>
Procedure	<p>A series of detailed steps to accomplish an end or instructions for implementation.</p> <p>A series of activities or tasks that contribute to the fulfilment of a task.</p>

Term	Definition
Record	<p>Any recorded information</p> <p>(a) regardless of form or medium, including any of the following:</p> <ul style="list-style-type: none"> <li>(i) Writing on any material;</li> <li>(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;</li> <li>(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;</li> <li>(iv) book, map, plan, graph or drawing;</li> <li>(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;</li> </ul> <p>(b) in the possession or under the control of a responsible party;</p> <p>(c) whether or not it was created by a responsible party; and</p> <p>(d) regardless of when it came into existence</p>
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event.
Should	A recommended action that should be implemented where possible but that is not mandatory.
Special personal information	<p>Personal information as referred to in Section 26 of POPI .This includes any elements or fields related to the following categories-</p> <ul style="list-style-type: none"> <li>(a) Religious or philosophical beliefs;</li> <li>(b) Race or ethnic origin;</li> <li>(c) Trade union membership;</li> <li>(d) Political persuasion or affiliations;</li> <li>(e) Health or sex life;</li> <li>(f) Criminal behaviour;</li> <li>(g) Biometrics; and</li> <li>(h) Personal information of children.</li> </ul>
Standards	A document that provides specific, low level mandatory controls that help enforce and support policies.
Third Party	A person or body that is a separate legal entity to EThekwini Municipality.
Threat	A circumstance or event that has the potential to exploit vulnerabilities and violate security.
Transfer	To exchange information or data with another party.



## 2. LIST OF ABBREVIATIONS

Abbreviation	Full term
CISO	Chief Information Security Officer
EThekwini	EThekwini Municipality
ICT	Information and Communications Technology
ISO	International Organisation of Standardisation
PI	Personal Information
POPI	Protection of Personal Information Act

## 3. Preamble

The Protection of Information Personal Act 4 of 2013 introduced certain conditions to establish minimum requirements for the processing of personal information. This policy is intended to govern information handling practices related to personal information at EThekwini. It is aligned with the Protection of Personal Information Act, 4 of 2013 (POPI). In the event of any ambiguity, the definitions, stipulations, and requirements of POPI and any related regulations will prevail over this policy.

The entire lifecycle of information is considered under this policy, including creation, collection, capture, recording, use, manipulation, storage, transmission, display, disclosure, analysis, linking, sharing, distribution, transfer, disposal, destruction, and any other purposes for which personal information may be used.,

## 4. PURPOSE

The purpose of this policy is to articulate EThekwini's position on information privacy and the protection of personal information during the course of its business operations, and therefore to:

- provide management direction and support for information privacy and the protection of personal information;
- set the requirements and expectations for information privacy;
- ensure that information privacy is considered for all new and existing business activities, projects, programmes, businesses, processes, technologies, products or research;
- guide the implementation of appropriate policies, standards, processes, procedures, and controls that are necessary to uphold the confidentiality, integrity, and availability of all personal information resources within EThekwini; and
- set out the roles and responsibilities that all employees have towards privacy

## **5. SCOPE OF THE POLICY**

This policy applies to all business units and support functions of EThekwini, all employees, and other stakeholders, regardless of legal jurisdiction or geographic location, who may process or have access to personal information because of their relationship with EThekwini.

It applies to the processing of all personal information records in any format or structure, either electronic or hardcopy, including but not limited to, those of former, existing, and prospective employees, customers, and other stakeholders.

## **6. OBJECTIVES OF THE POLICY**

The specific objectives of this policy are:

- to ensure that EThekwini's information systems comply with relevant laws and regulations, industry leading practices and recognised international standards on information privacy and the protection of personal information;
- to enhance and promote trust in the information handling practices at EThekwini;
- to preserve the integrity and quality of all personal information for which EThekwini is responsible; and
- to protect EThekwini and its stakeholders from the consequences associated with the inappropriate use of their personal information;
- to serve as a basis for the development and implementation of privacy standards and practices which uphold the rights of individuals as afforded them by the Constitution of South Africa and related legislation such as POPI.

## **7. PRIVACY FRAMEWORK**

The Privacy Policy will be supported by privacy standards, processes, and procedures. The privacy standards will be derived from the policy statements and provide the details of actions necessary to achieve the objectives of the policy statements. Compliance with supporting standards, processes and procedures is therefore mandatory.

This policy is valid from the "Effective Date" outlined herein and is valid until further notice. This policy may be revised at any time but should be reviewed at a minimum once every two years by the EThekwini Municipality Information Officer (in line with the EThekwini's policy review processes). However, in lieu of a review during any specific period, the current policy will remain in effect.

## **8. INDEPENDENT REVIEW**

An independent assessment of EThekwini Municipality's adherence to this policy and/or to POPI and associated regulations shall be performed periodically. This may be performed by Internal Audit, as part of an audit exercise or by independent consultants, dependent on the needs of EThekwini Municipality as determined by EThekwini Municipality management.

## 9. LEGAL AND REGULATORY REQUIREMENTS

This policy and all related standards, procedures and guidelines shall comply with legal and regulatory requirements, including guidance released by the Information Regulator from time to time.

## 10. REFERENCE DOCUMENTATION

This document is underpinned by the following:

Number	Reference	Name of the Regulation /Document
1	Regulatory Framework	Protection of Personal Information Act, 4 of 2013
2	Regulatory Framework	Protection of Personal Information Act Regulations
3	Regulatory Framework	Promotion of Access to Information Act
4	Regulatory Framework	Promotion of Access to Information Act, 2 of 2000
5	Best Practice	AICPA/CICA Generally Accepted Privacy Principles (GAPP)
6	Best Practice	ISO 29100 Information Technology – Security Techniques – Privacy Framework
7	Best Practice	ISO 27001 Information Technology – Security Techniques – Information Security Management Systems (ISMS) – Requirements
8	Best Practice	ISO 27002 Information Technology – Security Techniques – Code of practice for information security controls
9	EThekwini Policies/ Documents	ICT Policy
10	EThekwini Policies/ Documents	Information Security Policy

## 11. COMPLIANCE

EThekwini expects all employees and any other third parties to comply with this privacy policy and supporting standards, processes, and procedures. Failure and/or refusal to abide by this policy may be deemed as misconduct, may result in an investigation and/or disciplinary action against an individual, grounds for termination of a contract or refusal by EThekwini to enter into a contract. A claim of ignorance as to the existence and/or application of this policy shall not be grounds for justification of non-compliance.

If any provision of this policy is rendered invalid under law, such provision must be deemed modified or omitted to the extent necessary, and the remainder of this policy must continue in full force and effect.

Non-adherence to this policy must be promptly reported to line management and the EThekwini Information Officer, who will initiate an investigation into any potential contravention. Any employee or other third party who fails to comply with this policy may be subject to appropriate disciplinary and/or legal action.

## **12. ROLES AND RESPONSIBILITIES**

All privacy responsibilities across EThekwini Municipality must be defined, documented, and allocated.

The following roles and responsibilities associated with this policy are outlined below. These persons and functions shall be responsible for collaboratively giving effect to the organisational, operational processes and technology aspects required by EThekwini Municipality to drive privacy compliance throughout the organisation. More details on the specific roles, responsibilities, activities, and tasks related to privacy are defined and documented in the supporting Standards, Processes and Procedures as approved.

The Information Officer must review these roles and responsibilities on a periodic basis, and whenever there is a change in the legislative or regulatory landscape which may have an impact on privacy-related operations and activities or those associated with personal information, update the policy accordingly:

### **12.1 POPI Information Officer**

- 12.1.1 The POPI Information Officer derives his/her duties and responsibilities from section 55 of POPI, and in the case of EThekwini, this role is undertaken by the Deputy City Manager: Governance.
- 12.1.2 The POPI Information Officer is permitted to delegate these duties and responsibilities to a deputy information officer. This role is recognised at EThekwini as the Head: City Administration.
- 12.1.3 The POPI Information Officer must oversee compliance with the conditions for lawful processing of personal information as described in POPI and any associated regulations or international data protection laws, as applicable.
- 12.1.4 The POPI Information Officer will be responsible for providing strategic guidance to EThekwini about information privacy compliance.
- 12.1.5 The key responsibilities of the POPI Information Officer are to plan, develop, implement, manage, and lead an information privacy compliance programme and all associated activities.
- 12.1.6 The POPI Information Officer is responsible for the development, implementation, maintenance, monitoring of compliance to privacy policy, related standards, processes & procedures.

12.1.7 The POPI Information Officer must ensure that appropriate contacts with authorities, the Information Regulator, special interest groups and/or other specialist privacy forums and professional associations must be maintained.

## **12.2 CISO**

12.2.1 The CISO must ensure that EThekwini has adequate information security protocols to safeguard the confidentiality and integrity of the personal information that is processed Electronically by EThekwini.

12.2.2 The CISO must assist the POPI Information Officer with investigation of breaches to EThekwini's information security protocols.

12.2.3 The CISO will be responsible for establishing, leading, and managing the EThekwini Information Security Programme.

## **12.3 EThekwini Management**

12.3.1 Management has a responsibility to support all privacy efforts within the organisation and must discharge such responsibility through demonstrable commitment.

## **12.4 Employees, Contractors and Third Parties**

12.4.1 All employees (as defined in the Glossary) and any other third parties must take responsibility for protecting their own and EThekwini information privacy.

12.4.2 All employees and other third parties are bound by a duty of confidentiality for all personal information which they meet as a result of their relationship with EThekwini.

12.4.3 Any incidents, or suspected incidents, related to personal information, breaches of privacy or alleged non-compliance with this policy or POPI must be reported to relevant management and the EThekwini CIO immediately.

## **13. POLICY STATEMENTS**

The principles of information privacy contained within this policy are aligned with POPI requirements and other generally accepted privacy best practice. The policy statements below describe the principles for the protection and appropriate use of personal information

at EThekwini. They govern the collection, creation, capture, recording, use, manipulation, storage, transmission, display, disclosure, analysis, linking, sharing, distribution, transfer, disposal, destruction, and any other purposes for which personal information may be used, except as required by legislation and regulations.

### **13.1 Processing Limitation, Minimality and Consent**

- 13.1.1 All personal information collected and used by EThekwini must be done lawfully, reasonably and in a way which does not infringe on the privacy of any individual.
- 13.1.2 Only the minimal amount of information required for the purpose must be collected, stored, and used.
- 13.1.3 Consent to use personal information must be obtained, unless otherwise allowed by law, as far as possible, and evidence of this consent must be stored together with the information collected.
- 13.1.4 Individuals must be allowed to object to the use of their information before it is collected and at any time thereafter.
- 13.1.5 The EThekwini Information Officer must be notified if any objections to the use of personal information are received after collection of this information.
- 13.1.6 As far as possible, personal information must be collected directly from the data subject, unless otherwise allowed by law.

### **13.2 Purpose Specification and Retention**

- 13.2.1 At all times, personal information must be collected and only used for specific purposes that are linked to the business needs or interests of EThekwini.
- 13.2.2 The data subject must be aware of the information being collected and the specific purposes for which it is being collected.
- 13.2.3 Personal information must only be kept for such time as required for the specified purpose, as specified by the individual (where lawful), as specified by organisational rules, and as required by law.
- 13.2.4 Once personal information is no longer needed to fulfil the specific purpose it was collected for, it must be securely disposed of in such a way that prevents its reconstruction in an intelligible form.

- 13.2.5 In cases where personal information needs to be retained, archived, or kept for proof or evidentiary purposes, access to such records must be appropriately secured so that this information cannot be used for any other purposes.

### **13.3 Further Processing Limitation**

- 13.3.1 If personal information is to be used for a purpose other than the one that was specified at the time it was collected, consent from the data subject for the new purpose must be obtained prior to using the personal information for the new purpose.
- 13.3.2 In cases where personal information is anonymised to the extent that it is not possible to identify data subjects, then such information may be used for other purposes and data subject consent is not required.

### **13.4 Information Quality and Data Subject Participation**

- 13.4.1 EThekwini must take steps to ensure that all personal information under its control is complete, accurate, up to date, and not misleading.
- 13.4.2 EThekwini must ensure that data subjects are provided access to their personal information, as appropriate, so that they may correct or update it, or exercise any other rights that they may have under applicable information privacy or data protection laws.
- 13.4.3 EThekwini must ensure that a data subject's identity has been suitably verified before allowing them to gain access to, correct or update any personal information related to them.

### **13.5 Openness**

- 13.5.1 EThekwini must maintain a Promotion of Access to Information Manual that is in line with the requirements of the Promotion of Access to Information Act (PAIA) and POPI. This manual must notify individuals and the general public of EThekwini's information practices, that is, how it collects, uses, retains and discloses personal information.
- 13.5.2 The Promotion of Access to Information Manual must be made readily accessible and available to individuals.
- 13.5.3 At the point and time where personal information is collected, individuals must be made aware of:

- i. the purposes for collecting or using their personal information;
- ii. any consequences for failing to supply such information;
- iii. any laws which authorise such collection;
- iv. where information will be transferred to a third party;
- v. where information will be transferred across international borders; and
- vi. the rights that they have in terms of their personal information

### **13.6 Security Safeguards**

- 13.6.1 EThekwini must ensure that generally accepted or best practice technical and organisational controls are in place to protect all personal information for which it is responsible.
- 13.6.2 Information security controls which support privacy and the protection of personal information must be evaluated periodically to ensure that they are operating effectively and to identify areas for improvement.
- 13.6.3 All third-party service providers and employees providing services to EThekwini and/or who have access to personal information must adhere to security safeguards which are aligned with those described in the EThekwini Information Security Policy and related standards. These safeguards must be documented in the form of a written agreement. Any such agreements must allow EThekwini to reserve the right to review the information security practices and procedures of any third party at any time and make provision for changes or updates to any agreement between EThekwini and such third parties.
- 13.6.4 If personal information is compromised, the POPI Information Officer must ensure that an investigation is conducted to determine the root cause, determine the impact to EThekwini and recommend corrective actions to deter future occurrences. The POPI Information Officer must also inform the Information Regulator as well as any data subjects of any personal information which has been or is suspected to have been compromised.

### **13.7 Special Personal Information**

- 13.7.1 The use of any of the categories of special personal information must be appropriately considered in line with POPI requirements, and suitable security measures placed on such information.
- 13.7.2 Explicit consent must be obtained in a recorded form from any data subject, except where allowed by law, before special personal information is collected.



13.7.3 Where data subjects are minors (that is, under the age of 18), or adults who are not legally competent, consent must be obtained from their parent or legal guardian before special personal information is collected.

13.7.4 In such cases where special personal information must be collected for EThekwini to comply with other legal obligations (such as employment equity, occupational health and safety or other regulations), consent is not required but data subjects should still be informed of the purpose of collection.

### **13.8 Direct Marketing**

13.8.1 Should it be a business requirement, any direct marketing or external communication activities must adhere to EThekwini standards and the requirements of POPI, including, but not limited to:

- i. obtaining consent to market to individuals, particularly those with whom EThekwini has no pre-existing relationship;
- ii. providing individuals with a reasonable opportunity to object to the use of their information for such purposes; or
- iii. providing a mechanism for opting out of all marketing initiatives, the cost of which must be borne by EThekwini.

### **13.9 Automated Decision-Making**

13.9.1 No data subject may be subject to any decision, based solely on automated decision-making, which results in legal consequences for him/her, or which affects him/her to a substantial degree.

13.9.2 EThekwini must provide data subjects with a process whereby they may make representation about any decision made solely by an automated system or associated processing.

### **13.10 International / Trans-border Information Flows**

13.10.1 The transfer of personal information to third parties outside the Republic of South Africa is prohibited unless the transfer adheres to the requirements of POPI as set out in 14.10.2 – 14.10.4.

13.10.2 Personal information may only be transferred to legal jurisdictions which have similar data protection laws to POPI and as allowed by any regulations.

13.10.3 Where such laws do not exist, EThekwini must ensure that appropriate security safeguards are in place and that the organisation to which the information is transferred agrees to uphold the conditions of POPI. The EThekwini CISO must evaluate such transfers of information.

13.10.4 Where required by law, EThekwini must obtain approval (“prior authorisation”) from the Information Regulator for the transfer of information across South African borders. This is a mandatory legal requirement for all cases in which special personal information is affected.

#### **14. POLICY MONITORING AND EVALUATION AND POLICY REVIEW**

14.1. This policy is intended to ensure that the Municipality complies with the provisions of POPIA in a standardised manner through the adoption and execution of appropriate Standards. Adherence to the policy will result in the enhancement of the Municipality’s image and in ensuring that the Municipality is not sanctioned for non-compliance.

14.2. It is however recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this policy document. Where an update or amendment does not materially alter this document, such a change may be made administratively.

14.3. Any alteration or update which materially alters this document will be done through a resolution of a municipal Council meeting.

14.4. The policy will be monitored by the Head: City Administration and the DCM: Governance who will report to Council every 2 years regarding the policy. This Policy will be reviewed every 2 years or as and when required by Council resolution or legal requirement.

14.5. Internal Audit will subject to the Audit provisions undertake periodic audits to ensure compliance with the policy.

14.6 Breaches of this Policy will be dealt with in accordance with the Councillors’ Code of Conduct, the Code of Conduct for Employees, Council’s Internal Disciplinary Code.