



# **Information and Knowledge Management Policy**

**Department of Social Development**

**2020-2023**

## TABLE OF CONTENTS

<b>1</b>	Definitions of Terms
<b>2</b>	Legislative Framework
<b>3</b>	Preamble
<b>4</b>	Purpose
<b>5</b>	Objectives
<b>6</b>	Scope of Applicability
<b>7</b>	Principles and Values
<b>8</b>	Policy Statement
<b>9</b>	Approving Authority
<b>10</b>	Exceptions
<b>11</b>	Administration of the Policy
<b>12</b>	Accountabilities and Responsibilities
<b>13</b>	Effective Date of the Policy
<b>14</b>	Implementation
<b>15</b>	Monitoring Mechanisms
<b>16</b>	Enforcement
<b>17</b>	Policy Review
<b>18</b>	Policy Approval
	Policy Implementation Plan

## DEFINITIONS AND TERMS

Terms	Definitions
1) Accounting Officer	The Accounting Officer of a Department or Provincial Government in terms of the Public Finance Management Act No 1 of 1999 as amended.
2) Administrative value	Records having administrative value are considered useful or relevant to the execution of the activities that led to the creation of the record and during an audit of those activities.
3) Appraisal	Decision regarding requirements for preservation regarding each document/series of documents.
4) Archival value	Refers to the long-term use that records may have for purposes other than functional use.
5) Archives	Non-current records of enduring value that are selected for permanent preservation due to historical, financial, legal or administrative value
6) BAS	The Basic Accounting System that was developed in 1992 to cater for government's basic accounting needs. It assists government departments to manage their income and expenditure, and also provide standard and ad-hoc reporting.
7) Business	The business of the department refers to the department's service delivery and internal support activities.
8) Capturing	Refer to the process of transferring knowledge from one employee's mind into tangible resource such as text document.
9) Data	Set of elements gathered and stored for future use. The elements may include figures, pictures, images, etc.
10) Data Warehouse	Refers to a large store of subject-oriented, integrated data collected from a wide range of sources and used to support and guide management decisions. This data is then used to develop different reports which are distributed to various sections of the Department.
11) Department	Eastern Cape Department of Social Development

12)Document referencing	The process of allocating reference numbers to documents. This assists in uniquely identifying the document and this makes it easy to store and retrieve the documents.
13)Electronic Document Management System	A system that provides the ability to capture, describe and categorize, store and retrieve, share and re-use electronic documents regardless of specific format.
14)Electronic Documents and Records Management System	Electronic document and records management system aims to enable organizations to manage documents and records throughout the document life-cycle, from creation to destruction.
15)Electronic records	<p>Information generated electronically and stored by means of computer technology. It can consist of an electronic correspondence system and electronic records system other than correspondence systems. It can include but is not limited to the following:</p> <ul style="list-style-type: none"> <li>a. Email</li> <li>b. Electronic files (e.g. Microsoft Office documents, pdf documents, images etc.)</li> <li>c. Master and Transactional data generated from SDIMS, GIS, PERSAL, BAS etc.</li> <li>d. Audio-visual (Video clips, Audio files, Music files, DVD's CD's)</li> <li>e. Scanned documents (scanned manual documents and images etc.)</li> <li>f. Meta data</li> <li>g. Audit trail data</li> </ul>
16)Electronic Records Management System	A system that stores electronic records and supports the medium to long term information needs of an office. It provides functionality over and above that of an electronic document management system to preserve the security, authenticity and integrity of records to enable the permanent preservation of records.
17)Electronic Records System	This is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and meta data (background and technical information in respect of the information stored electronically) and in hard copy. All these components

	are defined as records by the Act. They must therefore be dealt with in accordance with the Act's provisions.
18) End user	The person utilising the information, computer equipment and systems of the Department.
19) Ephemeral	Term used to describe records with little archival value that can be destroyed after disposal authority has been obtained from the Provincial Archivist.
20) Executive Management	The Executive Management of the Department and could include the Accounting Officer, Deputy Director-Generals (DDG's)/Executive Management of the Department. This normally constitutes the Executive Committee of the Department.
21) Explicit Knowledge	Knowledge that has been articulated, codified, and stored in certain media. It can therefore be readily transmitted to others.
22) File Plan/ Filing System	Plan according to which an institution arranges and file its correspondence so as to serve the office's requirements for information retrieval optimally.
23) Financial value	Records with fiscal value are those that fulfil and document financial authorisations obligations, and transactions. They are often subject to audit and therefore must be kept for the time period that an audit can be initiated.
24) General Disposal Authority	Standing authority issued for series of records which are common to all offices, e.g. financial records, tenders and contracts, personal staff files.
25) Historical value	Some records have enduring value, even beyond what people might be able to see. The deeds of land and minutes of parastatal boards all have research value because they can show us the history of a piece of land or the history of a parastatal. Some records document significant historical events.
26) Information	Collection of raw facts from which conclusions can be drawn.
27) Information Classification	Refers to the process of organizing data into categories for its most effective and efficient use. A well-planned

	information classification system makes essential records easy to store and retrieve.
28)Information Management	It is the process that includes the collecting, collation, capturing, storing, retrieval and dissemination of information from external and internal resources.
29)Innovation	The process of transforming an idea, generally generated through research and development, into a new or improved product, process or approach which relates to the real needs of society.
30)Integrated Document Management	Set of methods and technology consisting of messaging and calendaring, imaging and scanning, file/document tracking, electronic document/ record management, workflow, search and retrieval functions, that is used to manage the classification, location, movement, security, auditing, retention and disposal of records in any format.
31)Intellectual Property	Describes the application of the mind to develop something new or original.
32) Knowledge	It is information that is contextual, relevant and useful to undertake action to solve a particular problem.
33) Knowledge Champions	The people appointed by the Department to promote, support, communicate and implement knowledge management initiatives within the Department.
34)Knowledge Harvesting	Process of capturing and transferring the knowledge in an expert's head into information assets that can be used to develop institutional memory.
35)Knowledge Management	It is the process of capturing and documenting an individual's knowledge and then sharing that knowledge within the organization and effectively using it to enhance the organisation's performance, productivity and effectiveness, also to increase the organisation's competitive advantage.
36)Knowledge Management Steering Committee	The governing body for guiding the program adoption and continuous improvement of knowledge management.

37) Knowledge Sharing	It is the practical learning and takes place in workshops, during team discussion or anywhere where knowledge is shared.
38) Knowledge Transfer	Dissemination of knowledge from one party to another by various channels and taking place in different ways such as learning, sharing and storytelling.
39) Knowledge Worker	Individuals whose work primarily focuses on knowledge creation at work.
40) Learning Organisation	An organisation that tries to develop its human resources to their full potential and uses learning as a means of improving its business performance.
41) Legal value	Records with legal value can often be subject to official actions such as subpoenas, investigations or lawsuits. Records with legal value contain evidence of a legally enforceable right or obligation of government. They must be made available if they are requested for litigation, meaning they cannot be destroyed once requested even if the records have met their scheduled retention period.
42) Member of the Executive Council	In relation to a Provincial Department, means the Member of the Executive Council of a province who is accountable to the provincial legislature for that Department.
43) PERSAL	The Personnel and Salary System used for central administration of the public payroll. PERSAL offers personnel administration, holds information in a database or over a million employees, and offers standard and ad-hoc reporting.
44) Personal Information	<p>According to the Personal Information Act No. 4 of 2013, means 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,</li> </ul>

	<p>religion, conscience, belief, culture, language and birth of the person</p> <ul style="list-style-type: none"> <li>b. Information relating to the education or the medical, financial, criminal or employment of the person</li> <li>c. Any identifying number, symbol, email 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</li> <li>f. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal contents of the original correspondence</li> <li>g. The views or opinions of another individual about the person; and</li> <li>h. The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person</li> </ul>
45)Record	A document, regardless of form or medium created, received, maintained and used by the Department or an individual in pursuance of legal obligations or in a business transaction of which it forms part or provides evidence.
46)Records Classification System	Classification plan for the arrangement, storage and retrieval of records. This includes a filing system for correspondence files, records control schedule for records other than correspondence files and a classification system for electronic records.
47)Records Management	Area of general administrative management concerned with achieving economy and efficiency in creation, maintenance, use and disposal of Departmental records throughout their life cycle and in making the information they contain available in support of the business of the Department.
48)Tacit Knowledge	This is knowledge that is personal, not easy to express and difficult to communicate to others and it resides in



	the individuals head and the person may not be aware that they have the knowledge.
<b>Acronyms</b>	
49)BAS	Basic Accounting System
50)CIO	Chief Information Office
51)CoP	Community of Practice
52)DPSA	Department of Public Service and Administration
53)ECDSD	Eastern Cape Department of Social Development
54)EDRMS	Electronic Documents and Records Management System
55)FTP	File Transfer Protocol
56)FTP	File Transfer Protocol
57)ICT	Information and Communication Technology
58)IM	Information Management
59)IP	Intellectual Property
60)ISO	Information Standards Organisation
61)IT	Information Technology
62)KM	Knowledge Management
63)KMSC	Knowledge Management Steering Committee
64)MEC	Member of the Executive Council
65)NARS	National Archives and Records Service
66)PARS	Provincial Archives and Records Service
67)PERSAL	Personnel and Salary System
68)RM	Records management
69)SDIMS	Social Development Information Management System

## **LEGISLATIVE FRAMEWORK**

The following publications govern the execution of the Information and Knowledge Management and were taken into consideration during the drafting of the policy:

- 1) Constitution of the Republic of South Africa, 1996 (Act No 108 of 1996)
- 2) Promotion of Administrative Justice Act No. 3 of 2000
- 3) Public Service Act No. 108 of 1994
- 4) The Protection of Information Act No. 84 of 1982
- 5) Promotion of Access to Information Act No. 2 of 2000
- 6) Protection of Personal Information Act No. 4 of 2013
- 7) National Archives and Records Service Act No. 43 of 1996
- 8) Provincial Archives and Records Services Act No. 7 of 2003
- 9) Electronic Communications and Transactions Act No. 25 of 2002
- 10) Control Objectives for Information and Related Technologies (COBIT) 5 2012
- 11) White Paper on Transformation of Public Service 1995 .
- 12) International Standards Organisation 27001 Information Security Standard
- 13) Minimum Information Security Standards (MISS) 1996

## **1. PREAMBLE**

- a) The Department needs to ensure that reliable electric records, information and knowledge are created and maintained over time as evidence of official business transactions for the purposes of accountability, business continuity and disaster recovery, as well as knowledge capturing, sharing, storing and dissemination.
- b) Research on the Information and Knowledge Management practice within the Department was conducted. It was found out that the management and protection of information as well as knowledge is not a priority in the Department. Therefore, information confidentiality, integrity, availability and knowledge harvesting is not maintained. Based on the findings of the research, it was concluded that there is a need for an Information and Knowledge Management Framework, which is inclusive of policies, business processes and procedure manuals to be implemented in the Department.
- c) The National Archives and Records Services Act requires that structured systems be managed in such a manner that the authenticity and reliability of the records, information and knowledge contained in those systems can be proven beyond any reasonable doubt. Furthermore, the information contained in these systems also constitutes public records that form part of the corporate memory of governmental bodies, and therefore, needs to be managed according to the same principles by which all other records are managed.
- d) The National Archives and Records Services Act also requires that governmental bodies must manage records contained in unstructured systems with an Integrated Document and Records Management System that consists of, amongst others, electronic document management functionality that supports the immediate operational requirements of an office by helping governmental bodies to exploit their information resources more effectively, and electronic records management functionality that supports the medium to long-term information requirements of an office by capturing electronic records and managing them according to records management principles.

- e) The increasing use of electronic systems by the Departmental officials to conduct their business has significantly changed the way that records are created and kept. Therefore, electronic records keeping poses particular challenges pertaining to security, integrity, availability and confidentiality.
- f) Some of the information management challenges and gaps are the lack of a central repository for electronic records from unstructured systems; since the Department has not implemented an Electronic Records Management System, personal information and other records are not stored at the registry and therefore, security, confidentiality and integrity is compromised; the Department is faced with litigations due to lack of information availability; and lack of commitment to capturing good quality data and monitoring thereof.
- g) Knowledge Management (KM) is comprised of (1) *tacit knowledge* which is knowledge that is personal, not easily shared or expressed, and (2) *explicit knowledge* which is knowledge that is articulated, codified and stored in certain media and is easily transmitted or shared with others. Knowledge Management is a powerful tool to ensure an effective, efficient, professional, highly productive and capable public service. The management of knowledge is an essential task for any organisation and it is critical for improving the competitiveness of the Department and the effective functioning thereof.
- h) Knowledge Management is a process, and its activities involve collecting, collation, sharing, packaging, dissemination and use of information in decision making. It also enhances the Department's operational efficiency towards effective service delivery. Through the successful implementation of Knowledge Management, the Department will be able to, amongst others, improve productivity, efficiency, effectiveness and quality service delivery while avoiding repetition of the same work/ or re-inventing the wheel and avoid repetition of mistakes.

## **2. PURPOSE**

This policy is aimed at providing guidelines for the requirements that must be met for information and knowledge to be considered as authentic and reliable record of the Department's activity. It documents the requirements for processes, technology and systems that create, capture, use and preserve the Department's electronic records. The policy is aimed at ensuring compliance with the regulations relating to the Protection of Personal Information Act No. 4 of 2013, published in the Government Gazette on 18 December 2018. Lastly, the policy provides for quality and reliability that must be maintained by the electronic record keeping process in order to ensure these records are retained as valuable information and knowledge resources for the Department.

## **3. OBJECTIVES**

This policy aims to ensure that the Department is compliant in the management of electronic records, information, personal information and knowledge throughout their lifecycle by managing and monitoring the following:

### **a) Creation, Collection and Capturing of information and records**

To ensure that the Department's information resources, are cost efficiently and effectively created, captured, filed and stored.

### **b) Information and Records Classification**

To ensure that electronic records are classified according to the Departmental classification system.

### **c) Use of information and records**

- i. To ensure that the Information Management unit provides timely and comprehensive information to meet daily operational business needs, accountability and legal requirements, and customer expectations.
- ii. To ensure provision of accurate and timely information to meet the management reporting requirements as well as support management in making better informed decisions.
- iii. To ensure that the Department properly addresses its information management challenges.
- iv. To ensure that personal information is processed and used for its intended purpose, having regard to the regulations of Act No. 4 of 2013.

**d) Retention of information and records**

- i. To ensure compliance to Section 13 (1) (b) (iii) in determining the conditions subject to which electronic records management systems must be managed.
- ii. To ensure the protection and availability of information to meet business continuity requirements;
- iii. To ensure the preservation of the Department's corporate memory through sound management practices and accurate capturing of information to meet legal, historical, evidential and accountability requirements.
- iv. To ensure that information is retained in compliance with applicable Provincial legislation.
- v. To ensure that personal information is not retained any longer than is necessary for achieving the purpose for which the information was collected or processed.

**e) Disposal of information and records**

- i. Section 13(2) (a)) of the Provincial Archives and Records Act No. 7 of 2003 states that electronic records may not be disposed of without the written authorisation of the Provincial Archivist.
- ii. Defining retention periods for information will ensure that records with functional, legal and historical value will be not be destroyed but preserved and protected until the time for archival or disposal arrives.
- iii. To ensure that personal information is disposed of in compliance with Act No. 4 of 2013 upon the Act being promulgated into law.

**f) Dissemination and sharing of knowledge**

Proper dissemination and sharing of existing knowledge, continuous learning, and cultural exchange within the Department, in order to enhance operational efficiency through the proper use of intellectual capital.

**g) Development of Knowledge Management System**

- i. The development of a comprehensive, efficient and effective knowledge management system, which will respond to the Department's programmes.
- ii. The development of an inventory of tacit knowledge, lesson learned and best practices through utilisation of reports from various Departmental sources.

- iii. The eradication of repetition of errors, mitigating the risks of reliance on an ageing workforce and to facilitate the goal of ensuring the right knowledge is available to the right people at the right time.
- iv. The accumulation and dissemination of knowledge base information for analysis and evidence based decision-making.
- v. The growth and preservation of department institutional memory.
- vi. All Departmental employees are empowered through capacity building to leverage the expertise of people across the organization.

#### **4. SCOPE OF APPLICABILITY**

This policy is applicable to all officials of the Eastern Cape Department of Social Development, internal and external stakeholders as well as oversight bodies. It covers all electronic data, information, personal information, knowledge and records regardless of format, medium or age.

a) The policy covers the following areas of information management:

- i. Information Ownership
- ii. Information and Records Lifecycle
- iii. Creation, collection, capturing and editing
- iv. Classification
- v. Use (Accessibility, Transmittal, Management)
- vi. Confidentiality, Availability and Integrity
- vii. Retention (Technology for information protection and storage)
- viii. Disposal (Archiving, Destruction)
- ix. ICT and Business Continuity
- x. Risk Management

b) The policy covers the following types of information:

- i. Electronic documents (scanned)
- ii. Correspondence
- iii. System generated master data: Employees, Beneficiaries, Clients, NPOs, Service Centres, Funded projects, CYCCs, CNDs, Assets, Inventory and any other information of a personal nature.
- iv. System generated transactional data: Transfers, General Payments, Procurement information such as Quotations, Requisitions, Purchase Orders, Invoices, Payment

Vouchers, Business plans, Claims, Inventory Management and any other information of a personal nature.

- v. Case Management information
  - vi. Community Development information
  - vii. Performance information including planning documents and reports
  - viii. HR Information
  - ix. Meta data
  - x. Audit logs
  - xi. Maps
  - xii. Research data
- c) Information security is out of the scope of this policy as it is covered within the approved Information Security policy of the Department.
- d) Data and information stored in transversal systems such as BAS and PERSAL is excluded as the ownership and management of data in these systems lies with the Provincial and National Treasury.
- e) The policy covers the following areas of knowledge management:
- i. Identification
  - ii. Capturing
  - iii. Analysis
  - iv. Organising
  - v. Sharing
  - vi. Re-use
- f) Tacit Knowledge: Personal ideas, beliefs, technical know-how etc.
- g) Explicit Knowledge: Documents, Books, Research Reports. Files, Procedure Manuals etc.

## **5. PRINCIPLES AND VALUES**

The principles, values and requirements are provided to ensure that information, knowledge and records management processes are integrated into business processes to enable information, personal information, knowledge and electronic records to be managed continuously throughout their entire life cycle.

- a) The Department shall recognise the value of the information and knowledge existing within the department and promote a culture of information and knowledge sharing.



- b) The Department shall take all precautionary measures to ensure information confidentiality, integrity and availability
- c) Information, knowledge and records generated by the Department shall be authentic, reliable, usable and have integrity.
- d) The Department shall comply with all legislative, regulatory and administrative requirements for information, knowledge and records management.
- e) The Department shall take appropriate measures to protect information, including personal information, which cannot be shared for reasons of security or privacy.
- f) The Department shall integrate its tangible and intangible assets to create the objective conditions required to structure an intelligent organisation, with ongoing learning capacity and of innovation.

## **6. POLICY PROVISIONS**

### **6.1 POLICY STATEMENT**

- a) The Department's information is a vital corporate asset, and the records of the Department are important sources of administrative, legal, fiscal and historical information. The Department's information provides evidence of the daily business transactions performed by both administration and core business. It also constitutes the Departmental corporate memory and provides a major platform for continuity and accountability.
- b) Information and records management operations are to be effected in line with approved policies, business processes, standard operating procedures and service standards of the Department. Each unit is responsible for making effective arrangements for managing the information and records relating to its functions, including the allocation of the necessary resources. Information management is a continuous process of risk assessment and risk management with the purpose of ensuring information confidentiality, integrity, and availability to its officials and management.

- c) Knowledge and Information about the services shall be accessible to all the stakeholders at the right time, in the right place and in the right format to maximise the effectiveness of the use and support of those services. A knowledge management system shall be created which will be used to coordinate the capturing, storing, processing, use and disposal of information and knowledge within the Department.
- d) Where possible, knowledge items shall be stored in the knowledge base provided within the service management system so that they are generally available to all officials. Opportunities to capture knowledge and make it generally available to those who need it should be actively sought and a culture of knowledge sharing should be encouraged.
- e) Re-use of knowledge should be supported where possible in the form of lessons learned reports, templates, checklists, pro-forma and other materials so that continual improvement is achieved. All knowledge items shall be reviewed at least annually in order to ensure that they stay accurate and complete. Access to services knowledge shall be controlled in line with the Department's security policies so that authorised people are able to view and manage it.

## **6.2 INFORMATION MANAGEMENT**

### **6.2.1 Information Ownership**

- a) The Department shall maintain an up-to-date list of authorised custodians of key information assets and records. All information and records collected and produced by employees, contractors and third parties in the course of their employment shall remain the Departmental intellectual property and must be managed according to the requirements of this policy.
- b) Employees and stakeholders shall obtain written authorization from the Accounting Officer for the use of Departmental administrative and other types of data, information and records for research and other purposes.

### **6.2.2 Information and Records Life Cycle**

- a) If proper life-cycle management is not implemented, records take up expensive space and it becomes impossible to retrieve important administrative, financial and legal and personal information.
- b) The Department must control records through the earlier stages of their life-cycle so that records that have low administrative value are not stored for too long and those of archival value can be identified and safeguarded.

### **6.2.3 Creation, Collection, Capturing and Editing of Information including Personal Information**

- a) The Department shall demonstrate compliance with the Public Records Act by meeting the mandatory requirements under section 27 requiring that public records are authentic, reliable, complete, comprehensive, usable and maintain integrity.
- b) Information and records shall be controlled, defined and have integrity so that they are fit for the purpose of their retrieval. All approved official documents shall be captured in a Departmental Electronic Documents and Records Management System (EDRMS) in accordance with the Departmental records management processes and standard operating procedures, and available for access unless there are valid business reasons for them to be withheld.
- c) The Department shall demonstrate compliance with the regulations relating to the Protection of Personal Information Act No. 4 of 2013, published in the Government Gazette on 18 December 2018.

### **6.2.4 Information and Records Classification**

- a) All staff shall ensure that there are consistent practices in naming, filing and describing documents and a standard classification system is used across the Department.
- b) By classifying records, the Department shall ensure that the public gain access to the right information at the right time and prevent access to information that should have been protected.

## **6.2.5 Information Use**

### **6.2.5.1 Accessibility**

#### **a) Access to electronic information and records**

- i. The Department shall develop business processes and standard operating procedures to ensure that all employees are aware of the information and knowledge management as well as electronic record keeping requirements and responsibilities and how to meet them.
- ii. Departmental electronic records shall be available to be shared within the Department unless they have legal or privacy constraints, security classification or there is a substantial business reason not to share.
- iii. To ensure the confidentiality, integrity and availability, the CIO Branch shall implement the necessary controls to manage access to electronic information and records.
- iv. The Department shall further ensure that all information and knowledge are stored in the appropriate media and easily accessible for use in order to support Departmental needs.

#### **b) Access by the Public**

- i. Records created and received by the Department and covered by the Public Records Act 2005 will be publicly and equitably available and accessible unless explicit reasons preclude. The Department shall make information available to the public as provided by the Promotion of Access to Information Act.
- ii. All staff shall ensure that there are consistent practices in naming, filing and describing documents and a standard classification system is used across the Department. By classifying records, the Department will ensure that the public gain access to the right information at the right time and prevent access to information that should have been protected.

#### **c) Access to Personal Information**

The Department shall develop a manual for accessing personal information as prescribed in the regulations relating to the Protection of Personal Information Act No. 4 of 2013, published in the Government Gazette on 18 December 2018.

**d) Management**

- a) Information and records are a strategic asset and resource of the organisation and must be effectively governed and actively managed throughout their lifecycle.
- b) The Department shall develop and maintain records and information management systems that capture and maintain records and information with appropriate evidential characteristics (e.g. meta-data and records classification).

**6.2.6 Confidentiality, Availability and Integrity**

- a) As part of managing information related risks, the Department must ensure that confidentiality, integrity and availability is maintained for all departmental information assets.
- b) The CIO employees, as well as all other Departmental employees who work with sensitive data, information, personal information and records shall be vetted or shall sign non-disclosure agreements.

## **6.2.7 Retention**

### **a) Preservation of electronic records and information**

- i. The Department aims to store most corporate information electronically to increase information accessibility and minimise unnecessary cost of paper.
- ii. In terms of the National Archives and Records Service of South Africa Act, governmental bodies are only obliged to transfer archival records into archival custody when they reach 20 years of age.
- iii. However, archival of electronic records cannot be left for 20 years before preservation actions are taken because technology changes so rapidly that the storage media outlast the software and devices needed to read the content on the storage media.

### **b) Security and Privacy**

- i. The Department needs practical means whereby the responsibility for electronic records can pass from the originator, to the people responsible for the corporate memory of the Department and then into the archival phase without jeopardizing the security, integrity and reliability of the records.
- ii. Information obtained from external stakeholders shall be protected and used in accordance with the provisions of this policy.
- iii. Personal information collected shall be protected and used in accordance with the regulations relating to the Protection of Personal Information Act No. 4 of 2013, published in the Government Gazette on 18 December 2018.

### **c) Technology**

- i. ICT systems developed to manage records shall comply with the Department's Enterprise Architecture, ICT Plan and the Infrastructure Management Strategy.
- ii. Records captured in the Departmental information systems shall be maintained in an accessible format for as long as they are required. These systems must include recordkeeping metadata.
- iii. Application software and source code of any system developed by external stakeholders or service providers, as well as data produced by those systems, regardless of the location where it is stored, shall remain the intellectual property of the Department.

### **6.2.8 Disposal**

#### **a) Archiving**

The archival of electronic records shall be managed by those authorized to do so as stipulated in the Records Management policy and performed according to the Records Management business processes and standard operating procedures.

#### **b) Disposal**

- i. No Personnel shall dispose of or delete Departmental or public information unless authorised to do so. Any official of the Department, who destroys records without the permission of the Accounting Officer commits an offence and may be subjected to internal disciplinary processes.
- ii. For data maintenance purposes, authorised officials may only mark the records for deletion and these records will remain in the database and wait for archival as per the retention period.

### **6.2.9 ICT and Business Continuity**

- a) All 'critical information' i.e. those without which the Department cannot continue to function are identified and particular attention is paid to their protection.
- b) Information management activities shall be directed towards ensuring business continuity and efficiency of services, operations and related Departmental outputs.

### **6.2.10 Risk Management**

- a) Information and records remain the intellectual property of the Department and no staff, internal or external contractor is not allowed to destroy or share information with any individual or organization unless mandated or authorised to do so by the Department.
- b) The Risk Manager shall ensure that all risks pertaining to information and records management, including unauthorized access and sharing of personal information are identified, recorded, assessed and mitigated or accepted by those assigned with their responsibility.

## **6.3 Knowledge Management**

### **6.3.1 Identify and Establish Partnerships**

- a) Internal Partnerships between Core Business, ICT unit, Monitoring & Evaluation unit, Communication Unit, Strategic Planning unit and District Municipalities as well as Local Government Municipality.
- b) External Partnerships with other Provincial Departments, National Departments and Provinces, Parastatals, Non-Government Organisations, and Institutions of Higher Learning.

### **6.3.2 Mainstream and Institutionalise Knowledge Management**

- a) Identify and appoint IKM Champions from all Districts and Provincial Office, therefore enabling different programmes to be represented in the IKM initiatives.
- b) Perform Information and Knowledge assessments or audits.
- c) Develop and implement Knowledge Management Strategy and incorporate the strategy into Departmental Operational Plans.
- d) Establish Knowledge Management processes.

### **6.3.3 Translate Individual and Organisational Learning into Organisational Intellectual Capital**

- a) Create an environment for employees to share ideas by encouraging knowledge sharing session by means of coaching and mentoring and CoP's.
- b) Ensure tacit knowledge is codified and transferred into explicit knowledge.
- c) Develop a knowledge base for the Department.
- d) Communicate service standards and raise awareness of KM processes and principles.
- e) Employees are encouraged to share research papers, reports, journals etc. by publishing these documents on the IKM Portal

### **6.3.4 Capture and Preserve Organisational Intellectual Capital**

- a) Develop the database and archiving system.
- b) Capture case studies, success stories and best practices.
- c) Sharing success and failures – story telling, brainstorming, exit interviews.
- d) Classification of packaged information.



- e) Maintain Master data files
- f) Capital archiving of document

### **6.3.5 Develop Institutional Information and Knowledge Management Portal**

- a) Implement interactive, user-friendly portal – e.g. intranet
- b) Develop data repository for frequently asked questions
- c) Create search engine for knowledge that is stored in the portal
- d) Establish information access control and security to protect intellectual property

## **7. APPROVING AUTHORITY**

The Accounting Officer and Member of Executive Council (MEC) shall approve this policy.

## **8. EXCEPTIONS/EXEMPTIONS**

Manual records are exempted from this policy as they are provided for within the Departmental Records Management policy.

## **9. ADMINISTRATION OF THE POLICY**

The Accounting Officer shall be responsible for the administration and enforcement of the policy.

## **10. ACCOUNTABILITIES AND RESPONSIBILITIES**

### **10.1 Member of the Executive Council shall:**

- a) Approve the Information Management policy.
- b) Ensure that Departmental policies are aligned to government strategic priorities.

### **10.2 Accounting Officer shall:**

- a) Assume the custodianship responsibility of Departmental policies.
- b) Ensure enforcement and proper implementation of this policy.
- c) Appoint IKM Champions.

**10.3. Chief Information Office shall:**

- a) Champion policy development and advocate policy implementation and evaluation within the Chief Directorate.
- b) Initiate new policy proposals that are consistent with government objectives and integrate cluster and provincial priorities.
- c) Organize, integrate and coordinate technical, organizational and human resources for effective implementation of this policy.
- d) Monitor policy implementation and provide feedback to Top Management on the implementation challenges and propose appropriate actions for the Department.

**10.4. Director Management Information Services shall:**

- a) Be responsible for the proper management and protection of information and records generated and stored within the Electronic Records and Document Management systems or other official systems developed
- b) Work in conjunction with the Deputy Director - Records Management to ensure that electronic records are properly managed, protected and appropriately preserved for as long as they are required for administrative, fiscal, legal and historical purposes.
- c) Ensure that all electronic systems capture appropriate metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created.
- d) Ensure that all data, metadata, audit trail data, operating systems and application software are backed to enable the recovery of authentic, reliable and accessible records should a disaster occur.
- e) Shall be responsible for the collection of all information and knowledge requirements and the development of Information Architecture as part of the Enterprise Architecture.

**10.5. Director Systems Development and Maintenance shall:**

- a) Develop, implement and maintain an Electronic Documents and Records Management System
- b) Ensure that appropriate systems technical manuals and systems procedures manuals are designed for each electronic system that manages and stores data, information, knowledge and records

- c) Ensure that Departmental systems are designed with functionality that improves the quality of data captured while providing excellent user experience
- d) Provide data capturing and processing training required for officials to properly manage information

**10.6. Director ICT Engineering shall:**

- a) Maintain acceptable levels of network and internet connectivity as per the ICT Plan
- b) Ensure that electronic data, information, knowledge and records are backed up daily and can be restored when required
- c) Provide the necessary storage for data, information, knowledge and records to ensure availability

**10.7. Deputy Director Information and Knowledge Management shall:**

- a) Implement the Department's Information and Knowledge Management policy and strategy.
- b) Facilitate the translation of individual knowledge to corporate intellectual capital (Institutional Memory).
- c) Develop and implement effective KM processes and systems and create information sharing platforms.
- d) Promote Knowledge Management in the Department by championing specific initiatives.
- e) Create and promote a learning culture for the Department.
- f) Translate user needs into KM requirements and conduct case studies and produce meaningful reports.
- g) Analyse the data to discover its real meaning or use and involve knowledge workers and data producers to clean data at its source.
- h) Capture and codify knowledge to facilitate its reuse.
- i) Coordinate Departmental Knowledge Management Forum and participate in the Records Management Forum.
- j) Lead information management processes including information sharing and systems review as part of core business processes.

**10.8. Deputy Director Data Warehouse shall:**

- a) Perform cleansing of all data sourced internally and externally before it is stored in the data warehouse.
- b) Backup all data, metadata, audit trail data, operating systems and application software on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.
- c) Perform regular data modelling checks and reports on all databases created by the Department to ensure compliance to the standards set in the approved data modelling standards document.
- d) Perform data quality checks on all master, transactional and other data captured and stored within the Departmental systems.

**10.9. Deputy Director Information Security shall:**

- a) Ensure that security is being considered when developing, testing, implementing and maintaining information management policies, procedures and systems.
- b) Ensure that electronic information and records are classified and only accessible to those who are duly authorised.
- c) Manage information risks.

**10.10. Security Management Unit shall:**

- a) Ensure that a comprehensive information classification system is developed and implemented by the Department.
- b) Ensure that all sensitive information produced or processed by the Department is be identified, categorised and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.

**10.11. Legal Services Unit shall:**

- a) Advise all Departmental policy custodians on technical and or legal correctness before approval by the Accounting Officer and the Member of Executive Council.
- b) Render legal advice to the Accounting Officer and the Member of the Executive Council in policy matters within the Department.

**10.12. Records Management Unit shall:**

- a) Be accountable for the record keeping and records management practices of the entire Department.
- b) Be responsible for the management of all records according to the records management principles contained in the Provincial Archives and Records Service Act No 7 of 2003, Eastern Cape.
- c) Determine the retention periods of electronic records in consultation with the end users and taking into account the administrative, legal, fiscal and historical need of the Department to maintain records of transactions.
- d) Make such training and other interventions as are necessary to ensure that the Department's record keeping and records management practices comply with the records management principles contained in the Provincial Archives and Records Service Act.
- e) Shall issue circulars and instructions regarding the record keeping and records management practices of the Department.
- f) Ensure that all records created and received by the Department are classified according to the classification system and filed according to the approved file plans.
- g) Ensure that a written disposal authority is obtained for them from the Provincial Archives and Records Service before any archiving or destruction of all records.
- h) Shall be responsible for keeping the policy custodian updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of the Department.

**10.13. Internal Audit Unit shall:**

- a) Internal Audit is authorized by Management to assess compliance with all corporate policies at any time.
- b) Internal Audit may assist with audits of the Information and Knowledge Management policy implementation, including testing and maintenance.

**10.14. Information and Knowledge Management Champions shall:**

- a) Act as information point of contacts within strategic Business units.
- b) Identify success stories for knowledge sharing.

- c) Collect best practise and provide information that is requested from their respective districts.
- d) Connect colleagues who need information with sources of appropriate information and knowledge inside and outside the Department and the province in general.
- e) Maintain information and knowledge connections with a variety of individuals and interest group – personally and through social media – act as conduits of information and knowledge dissemination for their colleagues.
- f) Participate in various communities of practice and fulfil knowledge brokering roles for colleagues in their divisions.

**10.15. Information and Knowledge Management Steering Committee shall:**

- a) Create a broad awareness of the perspective, purposes, and goals associated with the KM programme.
- b) Promote the sharing and integration of KM practices across the Department.
- c) Support KM champions.
- d) Provide leadership and resources for key KM initiatives and projects.
- e) Provide strategic direction for the adoption of KM within all Business units.
- f) Provide guidance that ensures that the overall and ongoing direction of KM is maintained.
- g) Forster communication and cooperation across the Department programme activities.

**10.16. Information Owner shall:**

- a) Ensure that all information generated by the unit is protected and managed as per the requirements of this policy and the Information Security policy.
- b) Monitor and ensure that the quality of data captured in the Departmental systems meets the standards set in this policy.
- c) Work with the Data Analyst to correct any data errors and as per the data quality reports received.
- d) Analyse BI reports received and correct any errors or inconsistencies found in the information.

**10.17. Data Analyst shall:**

- a) Perform data quality checks on system data before developing BI Reports

- b) Shall inform the data owner of any errors or inconsistencies found in master and/or transactional data
- c) Provide proper data analysis and advise the relevant programmes, sub-programmes and units of the steps to take to rectify any anomalies found.

#### **10.18. All Officials shall:**

- a) Implement Information and Knowledge Management policy at their respective levels.
- b) Adhere to policy statements, accountabilities and responsibilities in this policy.
- c) Play their role in the protection and management of Departmental information.
- d) Report any information security breaches and risks to the relevant unit.
- e) Be responsible to gather, organise and share their explicit and tacit knowledge.
- f) Define their key knowledge goals that align to the department objectives and goals.
- g) Continuously update their own profile in the expert / staff directory.
- h) Be encouraged to attend knowledge sharing sessions organised by IKM Champions and management.

#### **10.19. Responsibilities of the Policy Custodian**

The primary responsibility of policy custodians is to ensure the continued accuracy of the policies assigned to them by their units. Users across the Department rely on the policy manuals to provide accurate guidance, and regularly make important business decisions based on the information contained within the policy manual. Whenever the source document or related information for the policy section is updated, the policy custodian is responsible for reviewing the local policy manual section for compliance.

The Policy Custodian shall:

- a) Develop and implement this policy and procedures on behalf of the Accounting Officer within the requirements of the Departmental Policy Development Framework.
- b) Undertake appropriate consultation before submitting the policy and procedures to the Accounting Officer for formal endorsement / approval.

- c) Ensure that this policy is implemented and operationalized while ensuring compliance.
- d) Conduct reviews of policy and procedures in their designated areas, as required by the Departmental Policy Development Framework, to ensure that policies and procedures are accurate, widely understood and achieving their intended purpose.

## **11. EFFECTIVE DATE OF THE POLICY**

This policy shall be effective from the date of approval by the Member of the Executive Council and Head of Department.

## **12. IMPLEMENTATION OF THE POLICY**

- a) The policy custodian shall ensure the implementation of this policy over a period of three years from the date of approval as per the policy implementation plan.
- b) Deputy Director Knowledge Management shall ensure that the IKM processes and procedures are implemented and standardised.
- c) The Chief Directors shall provide the necessary tools of trade to ensure information and knowledge management as per the provisions of this policy.
- d) The Director ICT Engineering shall maintain acceptable network and internet connectivity levels to eliminate the use of Gmail and other external email accounts for work purposes. The Director Systems Development and Maintenance shall implement solution(s) to curb the current mail box limitation of 2MB which is limiting the use of internal email accounts. Once this is achieved as per the policy implementation plan, transmission of Departmental data, information and records using external email accounts shall be prohibited.
- e) Supervisors shall ensure the quality and completeness of all data and information collected from clients and stakeholders and captured within their units as part of their operational plan.
- f) All officials shall implement this policy by performing their responsibilities as provided in section 10 of this policy and by following the associated processes and standard operating procedures.



### **13. MONITORING MECHANISMS**

- a) The Management Information Services Directorate shall monitor the quality of electronic data and records captured in Departmental systems on a monthly basis and resolve any anomalies with data owners.
- b) Monthly and Quarterly Data Quality and System Utilization Reports shall be produced by the Business Intelligence Unit and used as a reporting mechanism.
- c) The IKM Champions shall monitor management of Information and knowledge at Districts and Provincial Office and report to the Management Information Services Directorate.

### **14. ENFORCEMENT**

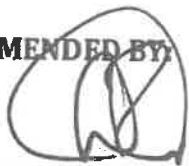
- a) The CIO Branch shall ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- b) Non-adherence to this policy may result in disciplinary action.

### **15. POLICY REVIEW**

To maintain its relevance, the policy shall be reviewed every three (3) years or when there is a directive or change in legislation.

**16. POLICY APPROVAL**

**RECOMMENDED BY:**



**DATE:**

26/02/2020

**MS N. BAART**

**ACCOUNTING OFFICER**

**DEPARTMENT OF SOCIAL DEVELOPMENT**

**APPROVED BY:**



**DATE:**

02/03/2020

**MRS. S.S LUSITHI**

**MEMBER OF THE EXECUTIVE COUNCIL**

**DEPARTMENT OF SOCIAL DEVELOPMENT**