

SOL PLAATJE MUNICIPALITY



Documents and Records Management Policy

*Approved by the Municipal Manager on 21 July 2011,
Reviewed: November 2019 in terms of
Council Resolution 298/10.*

Table Contents

1.	Definitions and Acronyms	2
2.	Policy Statement	5
3.	Legislative Framework	6
4.	Scope.....	6
5.	Access to Information Requests.....	7
6.	Record Keeping	7
7	Records classification systems and related storage areas	8
7.1	Correspondence systems	8
7.2	Storage areas	8
7.5	Special Guidelines for E-mail Records	10
8	Disposal of records	13
9	Storage and custody	14
10	Access and security	14
11	Legal admissibility and evidential weight.....	15
12	Roles and responsibilities.....	15
12.1	Municipal Manager	15
12.2	Executive Directors:.....	16
12.3	Records Manager	16
12.4	Chief Information Officer	17
12.5	Executive Director: Corporate Services.....	17
12.6	Executive Director: Financial Services	18
12.7	Registry staff.....	18
12.8	Employees.....	18
13	Training.....	18

1. Definitions and Acronyms

'Archives' means non-current records of individuals, groups, institutions, and governments that contain information of enduring value – in other words those records that no longer have an everyday use but are kept because of their historical value. They can be photographs, films, video and sound recordings, computer tapes, and optical disks, as well as unpublished letters, diaries, and other manuscripts.

'Archives repository' means the buildings in which records with archival value are preserved permanently.

'Authentic records' means records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.

'Authoritative records' means records that are authentic, reliable, trustworthy and useable and are complete and unaltered.

'Computer' means a computer belonging to the municipality; also includes laptops and tablet computers.

'Correspondence system' means a set of paper-based and electronic communications and associated documents, sent, received, generated, processed and stored during the conduct of business.

'Custody' means the control of records based upon their physical possession.

'Database' means a collection of information stored in a computer in a systematic way, and that can be accessed in different ways.

'Disposal' means the action of either destroying/deleting a record or transferring it into archival custody.

'Disposal authority' means a written authority issued by the National Archivist specifying which records should be transferred into archival custody or specifying which records should be destroyed/deleted or otherwise disposed of.

'Disposal authority number' means a unique number identifying each disposal authority issued to a specific office.

'Document' means any piece of written information in any form that is produced or received by an organisation or person. It can include databases, websites, email messages, MS Word and MS Excel files, letters and memos. Some documents will be of very short-term value and should never end up in a records management system.

'Document management' means the specific field of management that deals with the management of explicit unpublished knowledge resources in their editable phase. Document control entails all the measures taken to regulate the preparation, review, approval, release, distribution, access, storage, security, alteration, change, withdrawal or disposal of documents.

'Document management system' means an electronic system that is used to index, structure, store, version, retrieve and track electronic documents and/or images of paper documents. Functionality also includes logging an audit trail and applying document security

techniques. These systems allow documents to be modified and managed but typically lack the records retention and records disposition functionality for managing records.

'Electronic records' means information which is generated and stored electronically by means of computer technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

'Electronic records system' means a computer programme or a set of programmes designed to track and store records. This includes all other electronic media as well as all connected items such as source documents, output information, software applications, programmes and metadata (background and technical information in respect of the information stored electronically) and in hard copy.

'Email' means electronic mail (email or e-mail) is a method of exchanging digital messages from an author to one or more recipients over a network. In terms of this policy, "Email" refers specifically to email that has been generated, distributed or received by the municipality.

'Executive Director' means a senior manager appointed in terms of section 56 of the Municipal Systems Act (Act No. 32 of 2000).

'File plan' means a pre-determined classification plan by which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.

'Filing system' means the collective noun for a storage system (like files, boxes, shelves or electronic applications and storage systems) in which records are stored in a systematic manner according to a file plan.

'Municipality' means the Sol Plaatje Municipality.

'Non-archival records' means records with a short lived interest or usefulness.

'Public record' means a record created or received by a governmental body in pursuance of its activities, regardless of form or medium.

'Peripheral' means a device or part of a device that can be attached to and used with a computer. It can be a device that sends or receives data or instructions to or from a computer.

'Records management' means the process of ensuring the proper creation, maintenance, use and disposal of records throughout their life cycle to achieve efficient, transparent and accountable governance.

'Records other than correspondence systems' means records that do not form part of a correspondence file, or a case file e.g. registers, maps, plans, electronic records, audio-visual records, etc.

'Record' means

- (a) Recorded information regardless of form or medium.
- (b) Evidence of a transaction, preserved for the evidential information it contains.

'Records classification system' means plan for the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in the classification system.

'Recording' means anything on which sounds or images or both are fixed or from which sounds or images or both are capable of being reproduced, regardless of form.

'Record keeping' making and maintaining complete, accurate and reliable evidence of official business in the form of recorded information.

'Retention period' means the length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.

'Schedule of documents other than correspondence systems' means a control mechanism for documents other than correspondence files (other records), which contains a description and the disposal instructions and retention periods of all other records. It consists of the following parts:

- Schedule for paper-based records other than correspondence files;
- Schedule for electronic records systems other than the electronic correspondence system;
- Schedule for microfilm records;
- Schedule for audio-visual records.

2. Policy Statement

All public servants are required to create and preserve organisation records. Same is required of Sol Plaatje Municipality's (SPM) employees for all functions, policies, decisions, procedures and transactions. The records must be properly stored, preserved and be made accessible.

By managing its records effectively and efficiently the municipality strives to give effect to the actability, transparency and service delivery values contained in the legal framework.

- 2.1 The purpose of this policy is to facilitate the proper creation, management, preservation and disposal of records.
- 2.2 All employees of the SPM shall implement this policy.
- 2.3 All records created and received by the SPM shall be managed in accordance with the records management principles contained in the National Archives and Records Act of 1996.
- 2.4 The following broad principles apply to the record keeping and records management practices of the SPM:
 - (i) Following sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
 - (ii) Ensuring records management procedures of SPM comply with legal requirements, including those for the provision of evidence.
 - (iii) Following sound procedures for the security, privacy and confidentiality of its records.
 - (iv) Providing that email should be filed into the file plan as well as any attachments that meet these criteria.
- 2.5 Information requestor(s) outside the municipal employment or within municipal employment, acting in their own private capacity, or capacity as municipal employee(s) or on behalf of a public/private body or relevant authority(s), must follow the applicable process to request municipal information.

3. Legislative Framework

By managing its paper-based and electronic documents effectively and efficiently the Municipality strives to give effect to the accountability, transparency and service delivery values contained in the legal framework established by:

- The Constitution of South Africa, 1996;
- National Archives and Records Service of South Africa Act (Act No. 43 of 1996 as amended) (hereafter referred to as the National Archives Act);
- Municipal Finance Management Act (Act No. 56 of 2003);
- Municipal Systems Act (Act No. 32 of 2000 as amended)
- Municipal Structures Act (Act No of 117 of 1998 as amended)
- Promotion of Access to Information Act (Act No. 2 of 2000) (hereafter referred to a PAIA);
- Promotion of Administrative Justice Act (Act No. 3 of 2000);
- Electronic Communications and Transactions Act (Act No. 25 of 2002).

4. Scope

- 4.1 This policy applies to all employees of the SPM.
- 4.2 This policy also applies, in part, to an information requestor(s);
- 4.3 All records, that are business transactions, that approve/authorise an action, and contain guidance/advice/direction/recommendation(s); relate to projects and activities being undertaken with regard to internal and external stakeholders; represent formal business communication between staff and contain policy decisions, etc. - must be deemed to be public records by all employees and shall be managed and kept for as long as they are required for functional and/or historical purposes in accordance with the prescriptions of the National Archives Act;
- 4.4 Employees should be aware records are subject to the PAIA requests and legal discovery when a lawsuit is pending. Should the records, which are a subject of a PAIA request or legal discovery be deleted, the Municipality will face the risk of litigation.
- 4.5 Employees who wilfully contravenes management provisions in this policy will face disciplinary action.

5. Access to Information Requests

- 5.1 According to the Promotion of Access to Information Act (PAIA), the municipality must provide access to public records through a prescribed form by postal mail, fax or email.
- 5.2 According to PAIA, the accounting officer is responsible for the PAIA requests and provides for delegation of this function.
- 5.3 The prescribed form can be obtained from the municipal offices or downloaded from the municipality website www.solplaatje.org.za.
- 5.4 The requestor must complete all the mandatory fields as indicated on the form.
- 5.5 The requestor must adhere to all applicable conditions as presented on the form.
- 5.6 The form must be submitted to the office as indicated on the form.
- 5.7 The municipal manager or the delegated officer must ensure that records of information requests are kept. The municipality must maintain all record(s) pertaining to requests for information.
- 5.8 The municipal manager or delegated official must provide a written decision in reply to the request within 30 days of receiving the request.

6. Record Keeping

- 6.1 In the absence of an approved file plan, the municipality must follow a record keeping structure that allows for records to be uniquely identifiable, and easily accessible.
- 6.2 Each directorate must ensure that the record keeping structure is documented and communicated to the employees and/or public as applicable.
- 6.3 The following conditions must apply to the record keeping structure:
 - (a) Each directorate must publish an approved file structure for the directorate files;
 - (b) The file structure on paper must be able to be duplicated electronically or easily transferred to the electronic equivalent;
 - (c) The directorate must use a naming convention that allows the information to be accessible and easily identifiable:
 - Indexing

- Cross referencing
 - Classification
- (d) The directorate must document the naming convention in use. Example, naming of policies can include PolicyName_UniqueID_YearCreated (POL Electronic Records Management_2345_2019)
- (e) The municipality may provide a document naming standard to guide directorates on how to develop and document a file structure. The document naming standard will include naming conventions as in (c) and (d) above.

6.4 Third party records management

The accounting officer or delegated official must ensure that the maintenance, storage, and subsequent access to the records maintained on behalf of third party(s) is provisioned according to the agreement between the municipality and the third party(s).

7 Records classification systems and related storage areas

The Municipality has the following systems that organize and store records:

7.1 Correspondence systems

- 7.1.1 Paper-based records will be classified according to the record keeping guidelines as specified in paragraph 6.
- 7.1.2 Each employee shall allocate file reference numbers to all correspondence (paper, mail) according to the approved subjects in the file plan.
- 7.1.3 When correspondence is created / received for which no subject exists in the file plan, the records manager should be contacted to assist with additions to the file plan. Under no circumstances may subjects be added to the file plan if they have not been approved by the records manager.

7.2 Storage areas

- 7.2.1 Paper-based correspondence files are kept in the custody of-
- 7.2.2 The Central Registry or other approved sub-registries;
- 7.2.3 All paper-based correspondence system records that are not HR related are housed in the Central Registry, or other approved sub-registries.
- 7.2.4 All these records are under the management of the records manager who is mandated to ensure that they are managed properly.

- 7.2.5 The registry is a secure storage area and only registry staff is allowed in the records storage area.
- 7.2.6 Employees who need access to files in the registry shall place a request for the files at the counter and sign-off receipt thereof.
- 7.2.7 The registry shall be locked when registry is not in operation.
- 7.2.8 The Human Resources Registry
- (a) All Human Resources related records are housed in the sub-registry at HR. The general HR subject files as well as HR case files are under the management of the records manager who is mandated to ensure that they are managed properly.
 - (b) HR maintains a set of paper-based case files for each staff member. These files are confidential in nature and are housed in a secure storage area at HR Registry. The employee files are managed as part of the List of Series of Separate Employee Files that are maintained and managed by the document manager.
 - (c) These files exist only in paper-based format and the physical tracking of the employee files are managed with the file tracking system in the Integrated Document and Records Management System.
- 7.2.9 Financial Services Registry:
- (a) All financial services records and which borne from the implementation of all budget-related policies e.g. supply chain management records shall be housed in a sub-registry at Financial Services Directorate. The subject files are under the management of the records manager who is mandated to ensure that they are managed properly.

7.3 Records other than correspondence systems

7.3.1 Schedule for records other than correspondence systems

- (a) The records personnel maintain a schedule of all records other than the correspondence system. The schedule contains a description of each set of records other than the correspondence system and indicates the storage location and retention periods of these records regardless of format.
- (b) Should records be created/received that are not listed in the schedule, the records personnel in co-operation with the records manager should be contacted to add the records to the schedule.

7.4 Electronic systems other than the correspondence systems

- 7.4.1 The Municipality has a number of electronic document systems in operation which are not part of the correspondence system and that generate and stores public records (water accounts, levies etc).

7.4.2 The IT manager is responsible for the day-to-day maintenance of these IT systems.

7.4.3 The records maintained in these systems are under the control of the Corporate Services which is mandated to ensure that they are managed properly.

7.5 Special Guidelines for E-mail Records

7.5.1 Applicability of e-mails as records

- (a) E-mails that are evidence of the business transactions of the municipality are public records and shall be managed and kept for as long as they are required for functional and/or historical purposes.
- (b) E-mails that approve an action, authorize an action, contain guidance, advice or direction, relate to projects and activities being undertaken, and external stakeholders, represent formal business communication between staff, contain policy decisions, etc. should be managed as records and should be filed into the file plan. This Policy covers the e-mail message itself as well as any attachments that meet these criteria.
- (c) An e-mail message is a record if it:
 - (i) Contains unique, valuable information developed in preparing position papers, reports, studies, etc;
 - (ii) Reflects significant actions taken in the course of conducting business;
 - (iii) Conveys unique, valuable information about the Municipality's programmes, policies, decisions, or essential actions;
 - (iv) Conveys statements of policy or the rationale for decisions or actions;
 - (v) Documents oral exchanges (in person or by telephone), during which policy is formulated or other business activities are planned or transacted;
 - (vi) Adds to the proper understanding of the formulation or execution of the Municipality's actions or of the Municipality's operations and responsibilities;
 - (vii) Documents important meetings;
 - (viii) Facilitates action by the Municipality's officials and their successors in office;
 - (ix) Makes possible a proper scrutiny by the auditor-general or other duly authorized agents of the government;
 - (x) Protects the financial, legal, and other rights of the Municipality and of the persons directly affected by the Municipality's actions;
 - (xi) Approves or authorizes actions or expenditure;
 - (xii) Constitutes a formal communication between staff e.g. Correspondence or memoranda relating to official business;
 - (xiii) Signifies a policy change or development;
 - (xiv) Creates a precedent e.g. By issuing an instruction or advice; involves negotiations on behalf of the Municipality; or
 - (xv) Has value for other people or the Municipality as a whole.
- (d) E-mails that contain the following do not need to be filed:

- (i) Meeting announcements;
- (ii) Announcements of employees' absences or schedules;
- (iii) Changes in telephone numbers or office locations;
- (iv) Meeting arrangements that normally would have been done by telephone;
- (v) Copies of memoranda or text sent for information rather than action;
- (vi) Messages that have only temporary value such as a message that a meeting time has changed;
- (vii) Messages that contain no evidence of the MUNICIPALITY's functions and activities; or
- (viii) Duplicate information already documented in existing records.

7.5.2 Filing of e-mails

- (a) E-mails shall under no circumstances be isolated from the Municipality's records management systems. They shall be captured according to the guidelines specified in 6(iii). E-mails and attachments shall be captured as separate but linked records.
- (b) If an e-mail impacts on the work of a user and it complies with the criteria stated in paragraph 6.5.1, above, the e-mail shall be filed by the sender except if:
 - i) There is a person in a unit or project group to whom the responsibility for this task has been designated; or
 - ii) It is an e-mail received from outside the municipality in which case the recipient is responsible for filing it.

7.5.3 Disposing of e-mails

- (a) E-mails considered to be public records shall not be deleted or otherwise disposed of without a written disposal authority issued by the National Archivist.
- (b) E-mails filed to subject files in the file plan are covered by Standing Disposal authority and shall be disposed of according to the retention periods in that disposal authority.
- (c) Should an e-mail be received/generated for which an appropriate subject file does not exist in the file plan, the Records Manager should be contacted to add an appropriate subject to the file plan and to apply for disposal authority on that subject.
- (d) E-mails that are not public records may be disposed of after 12 months in terms of the National Archives and Records Service's General Disposal Authority or the Destruction of Transitory Records.

7.5.4 Creating reliable e-mail records

(a) Structuring an out-going e-mail

- (i) E-mails that are public records shall contain sufficient information to ensure that they are properly contextualized and that they are meaningful and accessible over time.
- (ii) Outgoing mail shall include the reference number of the subject folder in the file plan in the top right hand corner of the message box to

provide a contextual link to the business activity that supports the e-mail.

(b) Proper subject line

- (i) Subject lines are very important, since they indicate to a recipient what the message is all about. If subject lines are not used appropriately, the recipients may not realize the importance of the message and choose to read it later or not at all. Users shall allocate useful subject lines to e-mails.
- (ii) If a user receives a message with a senseless subject line and needs to reply to or forward it, the subject line should be changed to properly cover the subject of the e-mail before sending it off.

(c) Auto-signatures

- (i) Staff should always be contactable even if their e-mail systems are down. Auto-signatures shall be used and shall contain the following identifying information of a sender:
 - Name of sender;
 - Job-title of sender;
 - Name of Directorate, Sub-Directorate, Division and Section;
 - Name of the municipality;
 - Postal address;
 - Telephone number; and
 - Facsimile number.

(d) Attachments

- (i) If an outgoing mail includes an attachment, the attachment shall be filed into the file plan in the Records Management System before it is attached to the e-mail to ensure that it contains the following prescribed minimum mandatory metadata.
 - (a) File plan reference number;
 - (b) Record title: A sensible name given to it by the user;
 - (c) Author;
 - (d) Originating organization;
 - (e) Originating sub office;
 - (f) Record date; and
 - (g) Record type.
- (ii) Attachments shall be virus free.

(e) Language used in e-mails

- i) Official communications shall be approached in the same manner as a business letter, thinking it through carefully and using proper grammar and correct spelling.

(f) Capturing e-mail string

- (i) E-mail messages on a particular subject can become a string of replies until a matter is finalized. In such cases users shall:
 - Place all e-mails into the system separately as they occur and relate them to each other; or
 - Capture the final message – in which case user needs to make sure that the final message contains whole thread of the discussion.

(g) When to capture e-mails

- (i) Users shall capture official e-mails at the time of the action to ensure:
 - That the chronological order of the business transaction is clear; and
 - That the authenticity of e-mail is guaranteed.

8 Disposal of records

- 8.1 No public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior written authorization from the records manager who shall act on the directives of the National Archivist.
- 8.2 The National Archivist has issued Standing Disposal Authority for the disposal of records classified against the file plan. The records manager manages the disposal schedule.
- 8.3 The National Archivist issued Standing Disposal Authority of records other than correspondence systems. The records manager manages the disposal schedule.
- 8.4 Retention periods indicated on the file plan and schedule were determined by taking Municipality's legal obligations and functional needs into account. Should a staff member disagree with the allocated retention periods, the records manager should be contacted to discuss a more appropriate retention period.
- 8.5 Retention periods for non-archival records must be determined by the records manager of the Municipality in consultation with its users.
- 8.6 Disposal in terms of these disposal authorities will be executed annually.
- 8.7 All disposal actions should be authorized by the records manager prior to their execution to ensure that archival records are not destroyed inadvertently.
- 8.8 Non-archival records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions may not be

destroyed until such time that the Director: Corporate Services or Municipal Manager has indicated that the destruction hold can be lifted.

- 8.9 Paper-based archival records shall be safely kept until they are due to be transferred to the National Archives Repository. Transfer procedures shall be as prescribed by the National Archives in the Municipality's Records Management Policy.
- 8.10 All paper-based archival records must be kept for 20 years before being transferred to the Archives Repository.
- 8.11 Disposal schedules should be kept on file.

9 Storage and custody

- 9.1 See par. 7 for an identification of all document and records classification systems and their storage locations.
- 9.2 All documents shall be kept in storage areas that are appropriate for the type of medium. The National Archives and Records Services' guidelines contained in the Records Management Policy shall be applied.
- 9.3 Specific policies for the management of electronic storage systems are contained in the Information Systems Security Policy.

10 Access and security

- 10.1 Records shall at all times be protected against unauthorized access and tampering to protect their authenticity and reliability as evidence of the business of the Municipality.
- 10.2 Security classified records shall be managed in terms of the Information Systems Security Policy.
- 10.3 No staff member shall remove records that are not available in the public domain from the premises of the Municipality without the explicit permission of the records manager in consultation with the Director Corporate Services or the Municipal Manager.
- 10.4 No employee shall provide information and records that are not in the public domain to the public without consulting the Municipal Manager. Specific guidelines regarding requests for information are contained in the Promotion of Access to Information Act.
- 10.5 Personal information shall be managed in terms of the Promotion of Access to Information Act until such time that specific protection of privacy legislation is enacted.

- 10.6 No staff member shall disclose personal information of any member of staff or client of the Municipality to any member of the public without consulting the Municipal Manager first.
- 10.7 An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.
- 10.8 Records storage areas shall at all times be protected against unauthorized access, the following shall apply:
- (a) Registry and other records storage areas shall be locked when not in use.
 - (b) Access to server rooms and storage areas for electronic records media shall be managed with key access.

11 Legal admissibility and evidential weight

- 11.1 All records of the Municipality shall at all times contain reliable evidence of business operations. The following shall apply:
- 11.2 No records shall be removed from paper-based files without the explicit permission of the records manager.
- 11.3 Records that were placed on files shall not be altered in any way.
- 11.4 No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the records manager.
- 11.5 Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

12 Roles and responsibilities

12.1 Municipal Manager

- 12.1.1 The Municipal Manager is ultimately accountable for all the document management practices of Municipality.
- 12.1.2 The Municipal Manager is committed to enhance accountability, transparency and improvement of service delivery by ensuring that sound document management practices are implemented and maintained.
- 12.1.3 The Municipal Manager supports the implementation of this policy and requires each staff member to support the values underlying this policy.
- 12.1.4 The Municipal Manager shall designate a manager to be the records manager of the Municipality and shall mandate the records manager to perform such duties as are necessary to enhance document management including record keeping and

management practices of the Municipality to ensure compliance with legislative and regulatory requirements.

12.2 Executive Directors:

12.2.1 Executive Directors are responsible for the implementation of this policy in their respective directorates and shall ensure that:

- (a) they lead by example and shall themselves maintain good document management practices including record keeping and records management practices.
- (b) all employees are made aware of their document management responsibilities and obligations.
- (c) the management of documents including e-mail is a key responsibility in the performance agreements of all the staff in their units.

12.3 Records Manager

12.3.1 The Records Manager is responsible for:

- (a) the implementation of this policy;
- (b) staff awareness regarding this policy;
- (c) the management of all documents according to the document management principles contained in the National Archives and Records Service Act, 43 of 1996.
- (d) the determination of retention periods in consultation with the users and taking into account the functional, legal and the historical need of the body to maintain records of transactions.

12.3.1 The records manager is mandated to make such training and other interventions as are necessary to ensure that the Municipality's document management practices comply with the records management principles contained in the National Archives and Records Service Act.

12.3.2 The records manager may, from time to time, issue circulars and instructions regarding the record keeping and records management practices of the Municipality.

12.3.3 The records manager shall ensure that all records created and received by Municipality are classified according to the approved file plan and that a written disposal authority is obtained for them from the National Archives and Records Service.

12.4 Chief Information Officer

- 12.4.1 The chief information officer is responsible for the day-to-day maintenance of electronic systems that creates, processes, stores, transmits and disseminates electronic records, including the related hardware, software, and enabling peripherals.
- 12.4.2 The chief information officer shall work in conjunction with the records manager to ensure compliance to National Archives of South Africa Act No.43 of 1996 and PAIA for electronic records.
- 12.4.3 The chief information officer shall ensure that the integrity of any electronic records is accomplished through procedures such as test and restores, data migration, audit trail verifications, and audits.
- 12.4.4 The information officer will ensure the necessary provisions are made in system acquisitions contracts/agreements and system implementation for record storage and retention in line with applicable legislation.
- 12.4.5 The chief information officer shall ensure that all electronic systems capture appropriate systems generated metadata, system activity logs, and audit trail data for all electronic records to ensure that authentic and reliable records are created and to ensure adequate audit trails are available pertaining to the electronic record(s) that are stored.
- 12.4.6 The chief information officer shall ensure that appropriate systems, technical manuals and systems procedure manuals are available for each electronic system that manages and stores records.
- 12.4.7 The chief information officer shall ensure that electronic records remain accessible.
- 12.4.8 The chief information officer shall ensure that all data, metadata, audit trail data, operating systems and application software are backed-up as provisioned for to enable the recovery of authentic and reliable records.

12.5 Executive Director: Corporate Services

- 12.51 The Executive Director Corporate Services is accountable for:
- (i) the physical security of all HR related records since they fall under the corporate services and the custodianship of human resource management;
 - (ii) the management of all council records and its committees, including electronic records and recordings of Council proceedings and resolutions in accordance with a defined file structure.

12.6 Executive Director: Financial Services

- 12.6.1 The Executive Director Financial Services is accountable for the physical security of all budget-related and other records since it is part of his/her directorate.
- 12.6.2 The management of all records related to the implementation of the Supply Chain Management Policy such as procurement records; including the storage of all contracts.

12.7 Registry staff

- 12.7.1 The registry staff is responsible for the physical management and, security of the records in their care.
- 12.7.2 Detailed responsibilities regarding the day-to-day management of the records in the registry are contained in the Registry Procedure Manual.

12.8 Employees

- 12.8.1 Every employee creates records of transactions while conducting official business.
- 12.8.2 Employees shall therefore manage those records efficiently and effectively by:
 - (a) allocating reference numbers and subjects to paper-based and electronic records according to the file plan;
 - (b) sending paper-based records to the registry for filing;
 - (c) ensuring that records are destroyed/deleted only in accordance with the written disposal authority issued by the National Archivist

13 Training

- 13.1 The records manager shall successfully complete the National Archives and Records Management Course, as well as any other records management training that would equip him/her for his/her duties.
- 13.2 The records manager shall identify such training courses that are relevant to the duties of the registry staff and shall ensure that the registry staff is trained appropriately.

13.3 The records manager shall ensure that all staff members are aware of the records management policy and shall conduct or arrange such training as is necessary for the staff to equip themselves for their records management duties.

14 Monitor and review

14.1 The records manager shall review the record keeping and records management practices of the Municipality on a regular basis and shall adapt them appropriately to ensure that they meet the business and service delivery requirements of the Municipality.

14.2 Inspection by National Archives and Records Service.

14.3 The National Archives and Records Service is entitled to full and free access at all times to all records of the Municipality.

14.4 This policy shall be reviewed on a regular basis and shall be adapted appropriately to ensure that it meets the business and service delivery requirements of the Municipality.

15 Policy Approval

This Policy is approved in terms of **Council Resolution 298/10**, which delegated the authority to the Municipal Manager to approve administrative policies

Approved by



Mr T. M MABIJA
Acting Municipal Manager

25/11/2019

Date