



Molemole Municipality

ICT Policies and Procedures

IT-04-01 Data, Information and Records Policy

Document Name: Data, Information and Records Policy

Policy Number: IT-04-01

Version: 001

Document Information

Policy	Data, Information and Records Policy
Version	001
Policy Code	IT-04-01
File Name	M OL-IT-04-01-001 Data Information and Records Policy.doc
Manual	IT Policies and Procedures Manual
Section	04 Data and Information
Applicability	This applies to all users who create and use data of any form.
Situations	This template applies in all situations in which there is data, information or records that are created, maintained, stored and retrieved, including situations in which such data, information and records are required to be used as evidence.
Changes	V001 : Initial Version
Policy Owner	IT Manager
Policy Enforcer	IT Manager

1. Overview

1.1. General Purpose

Information and information resources are valuable assets of Molemole Municipality and they form an important part of the operation and management of the municipality.

This and other policies have been put into place in order to protect these and to promote integrity, security, reliability and privacy of the entire information infrastructure including the information and data it contains, the network, the computers and other access devices.

1.2. Background to this Policy

Most organisations keep a large amount of their records in electronic format as opposed to physical files.

Municipalities have been moving towards the implementation of electronic document repositories but all are required to maintain a physical Registry to keep information as required by the Archives Act.

There are many Acts and Regulations that specify the retention of particular records and it is a substantial exercise to comply fully with these acts. However, these acts are already required to be maintained whether these records are maintained in paper or electronic form, and the introduction of electronic records does not impact on the responsibilities.

The difference lies in the fact that whereas the paper records have been traditionally managed by the Registry within the municipality, the electronic records are managed by the IT Department, and thus the responsibility for compliance shifts in such cases.

It is important to understand when the IT Department will take over a responsibility for records management which was previously held by other departments.

Some records, such as email records, do not have a paper counterpart, since these are a product of the information age and are more regularly used than letters and faxes for communications in many cases. In terms of Green ICT Policies, such emails must not be printed unless absolutely necessary.

2. Scope

- 2.1. For the purpose of this policy we can consider all data, information and records to be collectively identified by the term "records", consisting of transactions, formal or informal, which are created, received, sent or stored by individuals within the municipality.
- 2.2. Our concern in this policy is with electronic records, since this is concerned solely with IT Policies, and this policy assumes the existence of other policies and procedures that are required to manage physical records such as the Registry function within the municipality.
- 2.3. South African legislation requires many types of records to be retained for future reference, and each type has different requirements in terms of storage and retention. This policy assumes that these record types are already identified and that policies exist for the handling and storage of these documents concerning the need to store these physically within the Registry.
- 2.4. This policy thus concerns only the electronic handling and storage of records, including "born-digital" records which commence from electronic sources, as well as those which may never be produced into electronic form. The assumption is made that whereas these are handled using electronic storage means, that the requirements for storage, retrieval and retention are the same as physical records.
- 2.5. This policy thus concerns the specific requirements associated with the handling of electronic records.
- 2.6. This policy applies to all personnel who handle electronic records of all forms, including those who have access to email services and who send and receive email messages.
- 2.7. This policy does not include the handling of physical records or other non-electronic formats (film, microfilm, cards).
- 2.8. This policy is related to the following policies:
 - IT-02-01 Acceptable Use Policy
 - IT-03-01 Email Use Policy
 - IT-04-02 Information Sensitivity Policy
 - IT-01-03 Register of Information Assets (to include information stores and databases)

- IT-09-01 Disaster Recovery Policy

3. Purpose of this Policy

- 3.1. The purpose is to provide internal regulation of all data, information and records maintained in electronic form within the municipality.

4. Applicability

- 4.1. This Policy is applicable to the following situations:
- Electronic data or records must be stored, archived or retrieved
 - Email must be stored or retained
 - Data and records, including email messages, must be deleted.

5. Definitions for this Policy

- 5.1. Reference must be made to the standard list of definitions included into the Policy Framework IT-01-01.
- 5.2. This policy document also defines the following specific items:
- **Data Record:** includes all information, data and records which are stored in electronic formats and which fall within the scope of this policy.
 - **Record Store :** an electronic filing system or archive in which records are retained. This may also include physical stores of electronic media such as tapes and CDs.
 - **(Data) Records Manager :** the IT person specifically responsible for Data Records in terms of this policy.

6. References for this Policy

National Archives Act (46 of 1996)

- 6.1. This Act identifies the responsibilities of government bodies, and the "records manager" responsibilities within each government body.
- 6.2. This also outlines the required approach to the handling of public records and the requirements to maintain these without destruction, deletion or erasure.

COBIT V4.0*DS11.2 Storage and Retention Arrangements*

"Define and implement procedures for data storage and archival, so data remain accessible and usable.

The procedures must consider retrieval requirements, cost-effectiveness, continued integrity and security requirements.

Establish storage and retention arrangements to satisfy legal, regulatory and business requirements for documents, data, archives, programmes, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication."

ECTA 2002 : Electronic Communications and Transactions Act (25 of 2002)

The concern is with Chapter III Part 1 of the Act, concerning the Legal Requirements for Data Messages. This covers the following areas:

- Legal recognition of data messages (legal force of information in data messages, including information referred to in messages)
- Writing (requirement for information to be "in writing" is covered for data messages which are subsequently available for reference)
- Signature (only advanced signatures acceptable as produced by accredited authentication provider, not required if the originator and intent can be inferred)
- Original (concerning whether the data message has been altered since originally produced – to satisfy the requirements of a record being the "original copy").
- Admissibility as evidential weight of data messages (evidential weight established in terms of reliability of generation, storage and communication of message, how integrity maintained, how originator identified and other factors, certified printouts are acceptable evidence).
- Retention (requirements for retention of records are satisfied by data records if information is accessible, in a suitable format, and

that originator and date and time of creation and transmission can be determined).

- Production of document or information
- Notarisation, acknowledgement and certification
- Other requirements
- Automated transactions

Another part of specific concern is Chapter IV concerning e-Government Services, which relates to records handled through electronic filing and issuing of documents.

King II Report

Organisations must identify and mitigate corporate risks.

There are risks associated with the failure to implement a policy concerning data, information and records, since these records are required by law in many situations, to support efficient and effective operation and may also be required as evidence to support claims of mismanagement and illegal activities.

ISO 17799

There are many areas in ISO 17799 in which there is reference to the effective management of data records as part of an information security infrastructure.

PAIA : Promotion of Access to Information Act

This Act requires that the municipality make specific information available to the public on request.

This primarily concerns information which is personal to the requestor and which is being requested formally.

The PAIA compliance document is required to identify how the municipality carries out its responsibility and specifically what information is available and how this must be obtained.

This will mostly concern information identified as Level 2 in the Information Sensitivity Policy (information which is private to individual stakeholders).

7. Policy on Records Management

- 7.1. A single person must be allocated the role and responsibility for Data Records Management who will then “own” and manage the terms of this policy. This person is responsible for all management of electronic records and will have delegated responsibility for electronic records, reporting into the “records manager” of the municipality as identified in the Archives Act.
- 7.2. All data records which are maintained by the municipality must be identified clearly in terms of the following:
- A specific unique coding structure that identifies each record uniquely, as well as grouping of related records (such as those linked to a project or department).
 - The coding must also indicate the version of the information where this is applicable.
 - The type of data record (according to the File Plan classification).
 - Whether the data is in raw form or is encrypted.
 - The format of the data record (including specific versions and names of the data record standards).
 - The retention requirements (when their retention expires and the actions to take when this occurs).
 - The proof of originality and non-tampering.
 - Sufficient metadata to support efficient access.
 - Location of storage – including specialised storage for sensitive data (as per Information Sensitivity Policy). This must include files and folders on archive servers, or the location of off-line and off-site archives.
 - Media on which stored and means of conversion if required (for example from older tape backups).
 - The risks associated with the loss of records for each type of record.
 - Where to obtain the keys and codes to decipher encrypted data which is retained.

- 7.3. In most cases the data records are stored in a format which is not directly accessible for viewing (such as TEXT files or CSV files). In such cases special consideration must be given to accessibility to appropriate data readers. The following must be addressed in these cases:
- What readers are available (such as dBASE III or equivalent programs required to access .DBF files).
 - The coding structure of the contents (ASCII, UNICODE, EBCDIC).
 - A list of suitable data readers or translators must be available for each type of data format. These must be stored in accessible locations together with any documentation and support utilities to enable their operation. Such readers are not subject to retention requirements and are required to be kept permanently.
 - These data readers may themselves become obsolete over time with changes in technology and these are also required to be subject to migration.
- 7.4. Public requests for information must be handled in terms of the PAIA document which the municipality must provide on its web site. The records management function must be able to provide the range of public information requests as identified in the PAIA compliance document.
- 7.5. Where public requests for information carry a charge for the provision of the information, this charging and associated billing and collection must be administered through the Records Manager.

8. Data Storage and Archiving

- 8.1. All data, records and information which is available in electronic form must be stored in an appropriate manner suitable to protect it and which provides efficient and reliable access.
- 8.2. For records which must be retained and which are stored on media or in formats which may become obsolete, a period review must identify records under risk of obsolescence and a plan must be put into place to migrate the records into more modern media and formats. This is particularly relevant for records that must be retained for very long periods (20-50 years) such as certain Occupational Health and Safety Records.

- 8.3. All sensitive information must be handled in terms of its sensitivity in terms of the Information Sensitivity Policy.
- 8.4. There must be two levels of data record storage. The first level must include information and records available on-line through normal search and retrieval methods. The second is for longer-term archives which are maintained off-line and possibly off-site and which have been copied to media in specific formats. This will include tape archives, DVDs and other forms.
- 8.5. In situations in which sensitive data is kept off-site, then suitable protections must be introduced to protect the information while off-site. The following recommendations apply for this situation:
- No labelling of the tapes or disk which may identify the owner or the contents. Simply a reference number which has meaning to the owner of the media.
 - The content must be protected by using names for files and folders which do not identify the contents.
 - Any sensitive information must be encrypted before being loaded into the archive media.
 - The media must be handled by an authorised archive provider which may include existing providers of archives of paper records.

9. Policy on Classification of Records

- 9.1. In the majority of organisations there are a substantial amount of data records. In order to satisfy the requirements for records to be accessible it is essential that such records are classified in a way which supports efficient and effective retrieval.
- 9.2. The classification and search processes must identify both on-line and off-line records.
- 9.3. The records management approach must support a well-defined classified structure which supports the access to relevant information and this must be based upon the File Plan of the municipality.
- 9.4. The principle of the classification must be that relevant information is always discovered if the data records have been classified appropriately, even if the queries to access information also produce irrelevant information at the same time.

- 9.5. The classification structure is applicable to all types and formats of documents including word processing documents, spreadsheets, email records, digital images, database records, transactions, scanned records and any other form of information which is stored in digital form.
- 9.6. Classification must include at least the following meta-data elements:
- Author
 - Sender
 - Date time Sent / Received
 - Type of Data Record
 - Classification in accordance with the File Plan of the municipality.
 - Location of original version (within file system or document management system or archive).

10. Policy on Deletion of Records

- 10.1. The general rule is that all data records are the property of the municipality and cannot be deleted under any circumstances. (This is the provision provided in the Archives Act in terms of public documents). This includes documents, transactions, emails, attachments, electronic conversations and in essence everything created and stored on a computer system or transmitted over a network from or to a municipal computer.
- 10.2. The exceptions to this will include
- Temporary documents prior to the completion of an original final version.
 - Sensitive information for which the paper record is the "original" and for which electronic copies are required to be destroyed immediately after printing. For these, permission must be obtained from the National Archivist before such destruction can take place.

11. Policy on Compliance with the Archives Act

- 11.1. All records which are currently under the provision of the Archives Act within the Registry must also be subject to this Act when they are stored in electronic form as data records.

- 11.2. All such records must be produced in paper form and handled through the Registry which keeps the "original" versions of all documents and records subject to this Act and that the electronic versions are always considered to be "copies" rather than the original.
- 11.3. All such copies are thus not subject to the Archives Act, and will be retained in accordance with the retention period as specified by the municipality for each type of record.

12. Policy on Records used for Evidentiary Purposes

- 12.1. All records which are required to be retained for possible evidentiary purposes must be stored in a way which minimises the possibility of tampering.
- 12.2. It is a core requirement of data records used for evidentiary purpose that they are available in their original form and are able to be found using normal access methods which do not require specialised knowledge.
- 12.3. All records required for use as evidence will be valued based upon:
- Compliance with the grounds for being an "original" copy.
 - Proof of non-tampering.
 - Electronic signatures verifiable from external authorities.
 - The means of storage and the protections of access to the retained records.
 - Audit trails that record any changes or new versions of retained records.

13. Policy on Record Retention to meet Legal Requirements

- 13.1. Each type of data record must be identified in terms of its retention requirements.
- 13.2. Where the retention is legislated, then the retention identified in the legislation is the minimum retention period which must be used.
- 13.3. Where there is no legislation in force, then the municipality must adopt guidelines on retention periods. These guidelines must be supported by experts in the respective field of the data records (such as finance, human resources, health and safety).

- 13.4. All data records must indicate the retention and the records management systems must support the identification of records which are beyond their minimum retention times. As required, this can be used to trigger the disposal of data records that are no longer needed.

14. Policy on Disposal of Records after Expiry of Retention Period

- 14.1. When the retention period is reached, data records may be subject to disposal or to long-term archiving.
- 14.2. Consideration must be given to records which may be of importance as part of the heritage of the municipality and which must never be destroyed.
- 14.3. When records are disposed of, this must be done so as to respect confidentiality and privacy of the information. It is unacceptable to simply provide tapes or CDs with information to a waste management company. All such media must be rendered useless before leaving the record storage area.

15. Policy on Disaster Recovery Provision

- 15.1. All electronic records must form part of a comprehensive disaster recovery strategy.
- 15.2. Provision must be made within backups and restore standards to accommodate the full recovery of all records within the records management storage for eventualities as identified in the disaster recovery strategy.

16. Forms / Registers

Records Register

- 16.1. This register forms part of the Information Assets Register.
- 16.2. This is a sub-register which will indicate each individual record and file and folder within the larger register and must contain all of the relevant information as identified in this policy.

17. Penalties

- 17.1. Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

18. Review and Audit

18.1. This policy will be reviewed every 3 years from the date of approval or should a need arise.

18.2. The enforcement of this policy will be audited as follows:

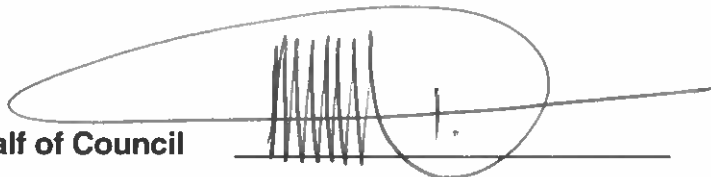
- Records retained in terms of the correct retention period and in the right manner.
- Records Register is up to date in terms of the actual record storage.
- The right information is maintained for each record.
- The records are classified in accordance with the File Plan.
- External archives are available on request and are accessible through authoritative requests only.

*** END OF DOCUMENT ***

a) Date of Approval by Council

29/05/2025

b) Signed on behalf of Council

A large, stylized handwritten signature in black ink, consisting of many vertical strokes and a long horizontal line extending to the right, is written over a horizontal line.