RECORDS MANAGEMENT POLICY

Policy Code: A12
Version: 1
Approved by: EXCO
Approval Date: 30/06/2021
Decision No.: EXCO38/2021

Date Reviewed	Version History
25/06/2021	V1

1. INTRODUCTION

The Da Vinci Institute is an accredited private higher distance education provider offering qualifications on NQF levels five to ten, which are registered on the Higher Education Qualifications Sub-Framework (HEQSF). This policy forms part of the institutional Integrated Quality Management System and details the principles for ensuring that programme offerings adhere to academic standards and empower students to contribute to the transformation of their communities, society, and the economy of the future. This approach is underpinned by the Business- and Community-based Action Learning discourse on the co-creation and distribution of relevant knowledge.

The Institute strives to achieve sound learning and quality assurance processes by managing its records in an accountable, effective and efficient manner through the implementation of records management processes that take into account related objectives such as orderly classification of records, retention and disposal, accessibility, security and confidentiality, and quality management of records.

Electronic records have the same status as paper records. Both electronic and paper records are bound by the same legislative requirements and are subject to the same degree of confidentiality and care.

2. ACRONYMS

CHE	Council on Higher Education
DHET	Department on Higher Education and Training
eLMS	Electronic Learner Management System
MIS	Management Information System
SAQA	South African Qualification Authority

3. DEFINITIONS

Term	**Definition**
Archives	Records relocated to long-term storage for preservation beyond their immediate business function, including permanent records
Compliance	Conforming to a rule, such as specified in the policies, standards, regulations or law. Regulatory compliance describes the goal that the institution aspire to achieve in their efforts to ensure that personnel are aware of, and take steps to comply with the relevant laws and regulations

Term	Definition
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information
Destruction	Destruction refers to the physical disposal of documents of no further value by shredding, pulping, etc.
Disposal	Actions taken with regards to records as a consequence of the expiration of their retention periods. Disposal is not synonymous with destruction. Disposal may involve one of the following activities: i. Transfer to a storage facility ii. Transfer of permanent records to archive
Electronic Records	Information that is generated electronically and stored by means of computer technology.
Evidence	All information that is presented to solve a problem and serve as grounds for the final decision.
Filing System	A storage system of boxes, folders, shelves, electronic storage systems, etc. in which records are stored according to a plan
Governance	The framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with all its stakeholders (financiers, customers, management, employees, government, and the community).
Information Security	The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
Record	Recorded information, regardless of format or medium, which has been created, received, used, accessed and maintained by The Institute as evidence and information in pursuance of its legal obligations or in the transaction of business. Included are e-mails, records in electronic format and records other than correspondence
Records Management	The systematic and consistent control of all records throughout their lifecycle.
Retention	The length of time that records should be retained before the disposal action is undertaken.
Retention Schedule	A report identifying the approved retention periods for records of an organisation. It establishes a timetable, outlining how long a record is kept and what happens to it through its lifecycle
Vital records	Records that are essential for the continuation of business and those records which protect the rights and interests of the institution, employees and students, including records relating to employee compensation and benefits, insurance, valuable

Term	Definition
	research findings, proof of ownership, financial interests, legal proceedings and decisions

4. REGULATORY FRAMEWORK

The Records Management Policy is benchmarked against and should be read in the context of the relevant legislation underpinning the principles against which institutional policies, processes and standard operational procedures are developed, implemented and maintained. These include:

A. Relevant legislation
   I. Companies Act (No. 71 of 2008)
   II. Constitution of the Republic of South Africa (No.108 of 1996)
   III. Electronic Communications and Transactions Act (No.25 of 2002)
   IV. Higher Education and Training Act 101 of 1997 as amended Act (No. 39 of 2008)
   V. National Education Policy Act
   VI. National Archives and Records Service of South Africa Act (No. 43 of 1996 as amended)
   VII. National Archives and Records Service of South Africa Regulations
   VIII. National Qualifications Framework Act (No. 67 of 2008)
   IX. Protection of Personal Information Act (No. 4 of 2013)
   X. Promotion of Access to Information Act (No. 2 of 2000)
   XI. Promotion of Administrative Justice Act (No. 3 of 2000)

B. Applicable Da Vinci documents:
   I. A4 - Privacy and Confidentiality Policy
   II. C1 - Electronic Information and Communication System Policy
   III. C2 - Acceptable Use of Information Policy
   IV. C3 - Information Security Management Policy
   V. C4 – Firewall Policy
   VI. C5 - Wireless Communication Policy
   VII. C6 - Change Management Information Technology Policy
   VIII. C7 - Incident and Service Management Information Technology Policy
   IX. C8 - Disaster Recovery Information Technology Policy
   X. C9 – Backup Policy
   XI. C11 - Data Breach Policy
   XII. PAIA Manual
   XIII. Records Retention Schedule

5. SCOPE

a) Records covered by this Policy relate to all recorded information and vital records used in relation to all aspects of the business of The Institute

b) The Records Management policy is applicable to all departments of The Institute.

6. PURPOSE

The purpose of this policy is to:

a) Inform all staff, whether full time or contracted, of the fiscal, legal and historical requirements on the creation, collection, usage, storage, maintenance, protection, archival, disposal and managing of information
b) Ensure confidentiality, privacy, security, integrity, accessibility and retrievability of all records.

The necessity for record keeping relates to:

a) Strategic business decisions based on information as per the Management Information Systems (MIS) of the institution
b) Keeping track of processes associated with the operational areas of The Institute
c) Enabling the prompt handling of both internal and external queries
d) Providing relevant reports and information to clients, departments, students, sponsors and stakeholders
e) Verification of activities associated with the day-to-day operations of The Institute
f) Verification of the integrity of teaching and learning processes and the quality assurance of activities in The Institute.

7. RESPONSIBILITIES

a) It is the responsibility of management to ensure that the necessary records keeping systems are in place to handle requirements associated with The Institute's core business focus of learning delivery. This responsibility is delegated to the personnel entrusted with the role and responsible for the execution of effective records keeping
b) Access to the various platforms is granted in accordance with *C3: Information Security Management Policy* and *C2: Acceptable Use of Information Policy*
c) The Institute has the responsibility to manage, store and retain certain documentation, records and other forms of information for specific periods for the following reasons:
    I. Sound corporate governance and records management practices
    II. Retention of documents and records for business/operational purposes as detailed in South African legislation
    III. Maintenance of evidence for possible future litigation, mediation, arbitration or disciplinary hearings
    IV. Processing student requests for information as detailed in the Promotion of Access to Information Act (PAIA) No. 2 of 2000
    V. Processing public requests for information as detailed in the Promotion of Access to Information Act (PAIA) No. 2 of 2000
    VI. The planning and implementation of the necessary systems to support the recording of core activities of education, training and development of The Institute, is regarded as a critical factor in the successful operation of business activities. This is to ensure the protection of the integrity of various processes associated with the management of education and training and

the resultant integrity of achievements and qualifications conferred to students registered with The Institute.

8. ROLES

8.1. Information Officer

The Information Officer is the Chief Executive Officer at The Institute who is responsible for:

a) Monitoring and maintaining a POPIA Compliance Framework
b) Ensuring that personal information impact assessments are performed
c) Process requests for access to personal information.

8.2. Deputy Information Officer

The Deputy Information Officers are the Information Technology Manager and the Registrar of The Institute, who must:

a) Develop and implement a POPIA Compliance Framework together with the Executive Committee
b) Facilitate the conduct of personal Information impact assessments
c) Develop and distribute a PAIA manual
d) Develop procedures and a system to process requests for access to personal information
e) Conduct internal awareness training
f) Monitoring and evaluating the process to ensure that departments are discharging their delegated responsibilities regarding information and records management
g) Facilitate the development of policies, processes, procedures and guidelines related to the management of information.

8.3. Executive Committee (Exco)

The Exco is responsible for:

a) Ensuring compliance with the Compliance Framework and related policies
b) Creating a culture and attitude of good information governance and management.

8.4. Information Technology Manager

The Information Technology Manager is responsible for:

a) Maintaining processes in support of this policy
b) Establishing appropriate controls and processes to ensure information related compliance
c) Establishing policies to ensure that the information assets and technologies are protected
d) The day-to-day maintenance of electronic systems that store records.

8.5. Staff

Staff are responsible and take ownership of record keeping within the context of standard procedures linked to their areas of operational input and output and will be held accountable for:

- Gathering of relevant data
- Recording of relevant data
- Maintenance of data
- Safekeeping of data
- Integrity and confidentiality of data.

9. TYPES OF RECORDS

9.1. Management Information System (MIS) Records

Records pertaining to students and their needs are used to inform key aspects of The Institute's strategic planning.

a) Student information is used to:
   I. Design programmes, courses, and materials
   II. Provide student support that is flexible and learner-centred.
b) The management information systems provide for:
   I. The tracking of student performance for example in assessments, examinations, or attendance at tuition support sessions or online workshops
   II. Identification of at-risk students
   III. Students who, though registered, are inactive
   IV. Determine pass and throughput rates
   V. Determine success rates of past and present students.

9.2. Legislative Records

a) Records and information as well as correspondence and communication whether in hard or electronic copy will be retained and filed in separate, uniquely identifiable files reserved for compliance purposes as an accredited higher education institution
b) The recording, maintaining, safe-keeping and back-up of such will be the responsibility of all the heads of The Institute.

9.3. Master Documents for Programmes

a) Master documents, records and information associated with specific learning interventions, learning programmes and qualifications utilised by The Institute whether in hard or electronic copy, will be retained and filed in separate, unique identifiable files reserved for this purpose
b) The recording, maintaining, safe-keeping and back-up of such will be the responsibility of the Design Office.

9.4. Staff Records

Staff records are kept by the human resources department. These include personal files, disciplinary records, performance appraisals and other relevant personal data of institutional staff.

9.5. Financial Records

a) Financial records pertain to staff and student finances, staff salaries, institutional finances and other confidential information of a financial nature.
b) Where applicable, relevant department heads will have access to departmental budgets and variance reports to enable the effective management of areas for which they hold responsibility and accountability.

9.6. Student Records

a) Student records pertain to student assessment and moderation information and examinations
b) The Institute utilises The Institute's MIS, which includes data from the eLMS and the LMS, for purposes of the recording of student information
c) Records filed, stored or archived shall be marked and indexed appropriately with the relevant information to enable identification and retrieval, and shall be kept locked away in a safe place
d) All records, electronic or otherwise, must be stored in a secure area with the necessary safeguards to prevent loss, unauthorised access and use, modification and misuse
e) Student registration data can be applied to the following potential reports:
    I. Number of student enrolments per programme or qualification
    II. Total number of enrolments for The Institute within a specific period
    III. Race and gender data as per meeting The Institute's commitment to access and redress
    IV. Dropout rates to measure success of interventions
    V. Student completion (throughput) rates.

9.7. Student Profiling Records

a) The Institute has developed a student profile that identifies the characteristics and situation of students projected to study by means of distance education.

    This profile includes:

    I. Demographic factors; age, gender, geographic location and occupation/employment if applicable
    II. Language profiles including language ability in main language of teaching and learning and language background
    III. Motivation for learning, for example, for career purposes or personal interest
    IV. Educational background/learning experience, for example, prior qualifications
    V. Special needs, for example, learning difficulties.

9.8. General correspondence

a) General institutional information will be received and forwarded to the relevant staff of The Institute
b) Incoming registered mail will be received and processed in accordance with the nature of the correspondence received
c) Outgoing mail will be recorded and handled by the designated administrative personnel, indicating the details of date of forwarding and the designated recipient
d) Faxes received from the designated fax area will be distributed as per the nature of the correspondence received
e) Internal correspondence to staff will be forwarded either in hard copy or via electronic internal mail. In some instances, personnel may be required to sign acknowledgement of receipt, or to sign an attached confirmation of receipt.

9.9. Other types of records

a) All other types of records will be subjected to the same requirements as outlined in this policy.
b) Other types of records refer to videos, film, sound records, photographs, pamphlets, maps, plans, registers, circulars, publications, financial records, etc.

10. RECORD KEEPING

a) The principles and procedures of record keeping apply to:

I. General administrative management
II. The development and standardisation of forms and templates used for administrative purposes
III. The utilisation of institutional forms and templates for the gathering of relevant information and data
IV. The recording, maintaining, safekeeping, back-up, recovery and protection of the integrity of data
V. Student administration management associated with all tuition, development, assessment, feedback, reporting and other operational activities
VI. The responsibilities associated with the data gathering processes and procedures
VII. Management of feedback and evaluation records
VIII. The regular update and maintenance of records to reflect any changes in legal and operational retention requirements
IX. Only institution-approved and legislation compliant paper-based filing systems and electronic-folder systems.

b) Core principles

I. The accuracy and integrity of data is non-negotiable and management takes full responsibility for:

a. The design and implementation of a functional administrative system and the relevant templates and formats for the sourcing of applicable records
b. The evaluation and review of information management and administrative systems to ensure that institutional needs are effectively met
c. The improvement of practices and procedures where non-compliance or lack of standardisation is evident
d. The necessary procedures, internal controls and review mechanisms that shall be introduced, applied and adapted by the institution to ensure meeting operational standards associated with the gathering, recording, maintaining and safekeeping of data for administrative purposes
e. The procedures that shall be developed for all actions pertaining to records keeping at The Institute. These procedures are linked to standard forms and templates.

II. The protection of information through controlled access is the right of The Institute in so far as it protects the interests of its clients and stakeholders in the provision of services forming part of the business focus of The Institute.
III. Proper care to be taken of the storage of inactive records
IV. The Institute quality assures the management of records and will take the necessary action where individual responsibilities in this regard are neglected or performance is inadequately executed
V. The verification of information is linked to maintaining accurate data and the necessary forms and templates for this purpose will be developed, utilised and evaluated with input from individuals responsible for specific operational areas
VI. Evidence collected for financial, personnel and learning activities is kept in accessed controlled files for reference purposes and is maintained on an on-going basis. Refer to *C3: Information Security Management Policy* and *C2: Acceptable Use of Information Policy*
VII. Data gathered can be used for the analysis of specific information enabling strategic planning in The Institute
VIII. It is the responsibility of all relevant parties of The Institute to gather appropriate information and data as per the required format at the identified intervals and timelines
IX. It is the responsibility of students to provide the appropriate personal information enabling the effective administration of training and development interventions
X. The Institute minimises the duplication of documentation through the use of a shared-drive and the linking of Management Information Systems
XI. All information relating to knowledge and intellectual property belonging to The Institute, students, alumni and staff shall be managed and stored in accordance with this policy

XII. Staff are required to complete the necessary forms and templates to the required institutional standards to enable the effective management of operational activities as it pertains to all operational areas in The Institute

XIII. Employees are to follow authorised institutional procedures in carrying out record management functions, and must observe security, privacy and confidentiality requirements at all times in accordance with this policy

XIV. Staff are required to report any data breaches in data security to the Information Officer or Deputy Information Officers. Refer to *C3: Information Security Management Policy* and *C2: Acceptable Use of Information Policy*

XV. Managers and their staff will ensure version control of documents. This will be achieved by indicating the version numbers on the documents and ensuring that the latest version of the document is in use.

11. RETENTION

a) All retained records will be legible, readily retrievable and stored in such a way as to prevent loss or deterioration
b) Information and evidence collected is electronically stored. This relates to student registration forms, assessments, student information, and the retention of records of final achievement
c) Records are stored in electronic, access-controlled repositories that are only accessible by the designated authorised personnel
d) Electronic records are removed/archived when appropriate
e) All final student records of achievement and records of certification are retained indefinitely and will be archived in electronic format
f) All records relating to the operation of The Institute will be electronically stored.

12. DESTRUCTION

Records are destroyed in line with agreed retention periods. Refer to The Institute's *Record Retention Schedule*. The destruction of physical documents is outsourced at The Institute and an agreement is in place regarding the secure destruction of the physical documents.

Destruction of records is authorised by staff with appropriate authority.

13. CONFIDENTIALITY

a) All information gathered for personnel records and information concerning student records are provided to The Institute in confidence. It is the responsibility of The Institute to ensure that the interest of the students and staff, as well as the preservation of confidentiality and privacy is attended to in a professional manner
b) The Institute will not avail any personal information telephonically
c) Any requests for any personal information must be placed in writing and written consent needs to be given by the subject
d) No employee of The Institute has the right to reveal institutional information, trade secrets or other information to third parties without the written permission to do so as obtained from the management of The Institute

e) The Institute retains the right to provide access to student data and records to stakeholders. Stakeholders are defined as the relevant quality assurance bodies, namely, the CHE, SAQA, DHET and employers and sponsors of training projects who have a vested interest in the performance, progress and conduct of students registered with The Institute for purposes of training and development
f) Students will be made aware of the necessity to avail records to the stakeholders listed in (e) above for purposes of verification, monitoring, auditing and where applicable, certification.

14. PROTECTION OF DATA INTEGRITY

a) All records will be identified, classified, retained, stored and protected in such a manner that its integrity is not compromised. In this regard, management ensures that processes and applicable technology are implemented to safeguard the integrity of records across the record lifecycle
b) Management with the assistance of legal counsel provide guidelines and processes to ensure that records are admissible evidence in courts or disciplinary proceedings notwithstanding the fact that such records were created, distributed, or stored in paper or electronic format
c) The Information Technology manager ensures that the necessary technology is employed to prevent the unauthorised access, tampering and destruction of electronic records
d) Employees may not disclose the nature and contents of any record to any person unless such disclosure is permitted in terms of the employee's job description, contract of employment, or upon written authorisation from the relevant manager
e) The integrity of data relates both to the initial data/information received or gathered in the normal operational processes at The Institute, and to the use, application and analysis of data/information resulting in relevant statistical analysis, reports and other forms of data application
f) Management of The Institute retains the right to request the validation of information received and to be utilised as source documents, in order to protect The Institute, its staff and students within the context of its operational parameters without unnecessarily infringing on individual rights to confidentiality, and as such has the right to request validation of:
    I. Evidence provided on entry of learning; latest educational level achieved, certified identity documents, certified copies of qualifications, confirmation of sponsorship, etc.
    II. Authenticity of evidence; contacting references in terms of evidence provided for purposes of awarding credits
    III. Any other reasonable validation required in the effective and professional conduct of institutional activities.
g) The integrity of applied data is maintained through access control and checks to ensure that the integrity thereof is maintained as effectively as possible. Refer to *C3: Information Security Management Policy* and *C2: Acceptable Use of Information Policy*.

15. DATA BACK-UP AND RECOVERY

a) The Information Technology department assuming the responsibility for electronic documentation control must ensure that data is secure in terms of control mechanisms including:
    I. Back-up and contingency functions
    II. Physical and data security
    III. Adequate measures in terms of virus and copyright violations.
b) All documentation and information back-ups and daily operational functions shall be executed on a daily basis
c) Technical information and support will be provided by technology staff with the relevant expertise to enable the protection of electronic data systems pertaining to firewalls, access control, document protection, and protection of any information utilised in electronic format.

16. ACCESS TO RECORDS

Inactive records are located in the institutional repository and may only be accessed by the designated authorised employees:

a) Records may only be copied and used, upon the written authorisation of the relevant department head
b) A record in the custody of The Institute must remain accessible to authorised individuals until final destruction
c) To ensure continued access to electronic records that are migrated across technologies and technology platforms, such migration must be undertaken in accordance with the relevant Information Technology policies
d) Individuals responsible for the gathering of specific information or data within the responsibilities associated with their job descriptions and particular areas of operation remain accountable for the gathering and safekeeping of such information
e) Employees are accountable for the securing, filing and recording of information as it pertains to their specified responsibilities
f) It is the responsibility of staff to ensure that relevant records are entered and/or updated expediently after receipt of updated information
g) Records may be password-protected enabling access only by the designated appointed personnel and management of The Institute
h) Only the relevant executive management and the human resources department will have access to personnel files, salary records, disciplinary records, performance appraisals and other relevant personal data of The Institute's staff
i) Only the applicable financial staff will have access to financial records as it pertains to student finances, institutional finances and other confidential information of a financial nature
j) Where applicable, relevant department heads will have access to departmental budgets and variance reports to enable the effective management of areas for which they hold responsibility and accountability
k) Applicable administrative staff will have access to student records as they pertain to student assessment and moderation information and final examinations

l) Access control procedures will be reviewed on an annual basis. Refer to *C3: Information Security Management Policy* and *C2: Acceptable Use of Information Policy*.

17. RECORD DISPOSAL AND DESTRUCTION

a) Paper or electronic records are not destroyed where litigation or audit investigations are pending or in process
b) Unauthorised destruction or disposal of records or information may result in criminal prosecution and/or disciplinary action and where applicable, liability of damages and losses incurred by The Institute and its clients.

18. REVIEW OF THIS POLICY

Regular review and amendment of this policy will be done in line with the approved institutional policies and regulatory requirements. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodian of this policy, namely the Registrar.