



POLICY: AI AND LARGE LANGUAGE MODELS

Policy Number	TM10
Version	1
Functional Area	Technology Management
Policy Custodian	Executive: Technology Management
Approved by	The Board
Decision Number	B.04.2026.49
Approval Date	01/10/2026
Effective Date	16/10/2026
Review Cycle	Annually
Next Review Date	01/08/2027
Version History	01/10/2026_v1

Table of Contents

1. INTRODUCTION.....	3
2. ABBREVIATIONS, DEFINITIONS AND TERMINOLOGIES.....	3
3. DEFINITIONS.....	4
4. REGULATORY FRAMEWORK.....	5
5. SCOPE	6
6. PURPOSE	6
7. PRINCIPLES.....	6
8. ACCEPTABLE USE OF AI	7
9. PROHIBITED AND RESTRICTED USES	8
10. DATA PRIVACY AND CONFIDENTIALITY OBLIGATIONS – ALL USERS	8
11. SPECIFIC DATA PRIVACY OBLIGATIONS FOR BOARD MEMBERS	10
12. STAFF AND MANAGEMENT DATA PRIVACY OBLIGATIONS.....	11
13. AI TOOLS, PROCUREMENT AND VENDOR DUE DILIGENCE	11
14. PROCESSING PERSONAL INFORMATION WITH AI.....	12
15. ACCURACY, BIAS AND HUMAN OVERSIGHT	12
16. INTELLECTUAL PROPERTY, COPYRIGHT AND CONFIDENTIAL KNOW-HOW	13
17. AI MEETING RECORDING, TRANSCRIPTION AND SUMMARISATION	13
18. SECURITY INCIDENTS, DATA BREACHES AND MISUSE.....	13
19. ROLES AND RESPONSIBILITIES.....	14
20. TRAINING, AWARENESS AND USER ACKNOWLEDGEMENT	15
21. MONITORING, RECORDS AND AUDIT	15
22. BREACH, NON-COMPLIANCE AND DISCIPLINARY ACTION.....	15
23. REVIEW OF THIS POLICY.....	15

1. INTRODUCTION

The Da Vinci Institute (The 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- driven Action Learning discourse on the co-creation and distribution of relevant knowledge.

Artificial Intelligence (AI), including generative AI and large language models (LLMs), can support productivity, teaching, learning, research, administration, and decision support. These technologies also create material risks relating to privacy, confidentiality, cybersecurity, intellectual property, accuracy, bias, records management, and accountability. The Institute therefore requires AI to be used lawfully, ethically, securely and with appropriate human oversight.

This Policy establishes mandatory governance requirements for Board members, Board and committee participants, executives, management, employees, faculty, contractors, and other authorised users. It places particular emphasis on the protection of personal information and confidential institutional information when AI tools or services are used.

2. ABBREVIATIONS, DEFINITIONS AND TERMINOLOGIES

Acronym	Meaning
AI	Artificial Intelligence
DIO	Deputy Information Officer
IO	Information Officer
LLM	Large Language Model
POPIA	Protection of Personal Information Act, No. 4 of 2013
SaaS	Software as a Service
TM	Technology Management

3. DEFINITIONS

Term	Definition
Approved AI Service	An AI system, application or service that has been approved by The Institute for the relevant use case and risk level.
Artificial Intelligence (AI)	Computer-based systems, software or services that perform tasks normally associated with human intelligence, including analysing, predicting, classifying, recommending, generating, or transforming content.
Board Information	Information contained in or associated with Board and committee packs, agendas, minutes, resolutions, strategy papers, financial reports, risk reports, legal advice, executive matters, personal information, investigations, and other governance records.
Confidential Information	Non-public information relating to The Institute, its students, employees, Board members, partners, suppliers, research, finances, systems, intellectual property, strategy or operations that requires protection from unauthorised disclosure.
Generative AI	AI capable of generating new text, images, audio, video, software code or other content in response to prompts or other inputs.
Large Language Model (LLM)	An AI model trained on large volumes of language data and capable of producing, analysing, transforming, or summarising natural-language content.
Personal Information	Personal information as defined in POPIA, including information relating to an identifiable natural person and, where applicable, an identifiable existing juristic person.
Public AI Service	An AI service made generally available to the public or accessed through a personal/free account where The Institute has not approved the contractual, privacy, security and data-processing arrangements.

Restricted Information	Information whose unauthorised disclosure, alteration or loss could cause material harm, legal or regulatory exposure. This includes special personal information, authentication credentials, highly confidential Board information, disciplinary or investigation records and legally privileged material.
Special Personal Information	Special personal information as defined in POPIA, including information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and criminal behaviour, subject to POPIA.
User	Any person within scope of this Policy who accesses or uses an AI system for Institute-related activities.

4. REGULATORY FRAMEWORK

This Policy is benchmarked against and should be read in the context of the relevant legislation, governance requirements and internal policies applicable to the Institute. These include:

4.1 Relevant legislation and recognised frameworks

- I. Constitution of the Republic of South Africa, 1996
- II. Higher Education Act, No. 101 of 1997, as amended
- III. Companies Act, No. 71 of 2008
- IV. Copyright Act, No. 98 of 1978, as amended
- V. Cybercrimes Act, No. 19 of 2020
- VI. Electronic Communications and Transactions Act, No. 25 of 2002
- VII. ISO/IEC 27001:2022 – Information security management systems
- VIII. ISO/IEC 42001:2023 – Artificial intelligence management systems
- IX. Promotion of Access to Information Act, No. 2 of 2000
- X. Protection of Personal Information Act, No. 4 of 2013
- XI. South African National AI Policy Framework (2024), as non-binding policy context where relevant.

4.2 Applicable Da Vinci documents

- I. PM24: Privacy and Confidentiality Policy
- II. TM7: Records Management Policy
- III. TM1: Acceptable Use of Information Systems Policy
- IV. TM2: Information Security Management Policy
- V. TM3: Change Management Information Technology Policy
- VI. TM4: Incident and Service Management Information Technology Policy
- VII. TM5: Disaster Recovery and Backup Policy
- VIII. TM6: Data Breach Policy.
- IX. TM9: IT Asset and Acquisition Policy

- X. Applicable academic integrity, research ethics, assessment, and intellectual property requirements.

5. SCOPE

This Policy applies to the use of AI for Institute-related purposes by:

- a. Members of the Board and members of Board committees or governance structures
- b. Executives, managers and all employees, whether permanent, temporary or fixed-term
- c. Faculty, researchers, facilitators, markers, moderators, and other academic personnel
- d. Contractors, consultants, interns, volunteers, and third-party service providers where they use AI in connection with Institute information, systems, or services
- e. Any other person specifically authorised to use AI on behalf of The Institute.

Student academic use of AI may also be governed by separate academic integrity, assessment, and research requirements. Staff who process student information through AI remain subject to this Policy regardless of any separate student requirements.

6. PURPOSE

The purpose of this Policy is to:

- a. Enable responsible and beneficial use of AI while managing legal, privacy, cybersecurity, academic, ethical, operational, and reputational risks
- b. Protect personal information, confidential information, Board information, intellectual property, and institutional records
- c. Define mandatory privacy and confidentiality obligations for Board members and all staff when using AI
- d. Ensure that AI-assisted decisions remain subject to appropriate human judgement, accountability, and oversight
- e. Establish requirements for the approval, procurement, use, monitoring and review of AI services
- f. Provide clear rules for reporting AI-related incidents, security compromises, inaccuracies, and misuse.

7. PRINCIPLES

Principle	Requirement
Human accountability	The person using AI remains accountable for the prompt, source information, decision, communication, and final output. AI does not assume accountability on behalf of a user, manager, executive or Board member.

Privacy and data protection by design	Only the minimum information reasonably necessary may be processed through AI, and personal information must be handled in accordance with POPIA and the Institute's privacy requirements.
Confidentiality and security	Institutional information must be protected according to its sensitivity. Public or unapproved AI services may not be used for confidential or restricted information.
Transparency	AI use must be disclosed where required by law, policy, academic integrity, professional standards or where disclosure is necessary to prevent misleading others.
Accuracy and verification	AI-generated outputs must be reviewed for factual accuracy, completeness, context, bias, fabricated references, and appropriateness before use.
Fairness and non-discrimination	AI must not be used in a manner that unlawfully discriminates, unfairly profiles individuals, or produces unjustified adverse effects.
Proportionality	The level of governance, approval and oversight must be proportionate to the sensitivity of the information and potential impact of the AI use case.
Lawful and ethical use	AI use must comply with applicable law, Institute policy, contractual obligations, intellectual property rights and professional or academic requirements.

8. ACCEPTABLE USE OF AI

- a. Users may use approved AI services for legitimate Institute purposes where the use is consistent with this Policy. Examples may include:
- b. Drafting, editing, summarising, or restructuring non-confidential business content, subject to human review.
- c. Generating ideas, outlines, checklists, training materials or administrative support content.
- d. Analysing non-sensitive datasets or information where the data has been appropriately anonymised or approved for the AI service.
- e. Supporting software development, troubleshooting and documentation where no credentials, secrets, restricted code, or protected data are disclosed.
- f. Supporting research, teaching, and learning where academic integrity, research ethics, copyright and disclosure requirements are followed.
- g. Assisting with meeting notes or summaries where the recording/transcription and data-processing requirements in this Policy are met.

All AI outputs remain draft or advisory until appropriately reviewed and accepted by an authorised human user.

9. PROHIBITED AND RESTRICTED USES

Unless specifically authorised in writing for an approved use case and approved AI environment, users must not:

- a. Enter, upload, paste or otherwise disclose passwords, multi-factor authentication codes, API keys, private keys, security configurations or other authentication secrets into an AI system.
- b. Upload personal information, special personal information, confidential information, Board information, student records, employee records, disciplinary information, health information, financial account information or restricted institutional records to a public or unapproved AI service.
- c. Use personal AI accounts to process Board packs, committee papers, Institute confidential information or work-related personal information.
- d. Use AI to impersonate another person, fabricate evidence, create deceptive records, conceal misconduct, bypass security controls, or engage in unlawful activity.
- e. Use AI as the sole decision-maker for recruitment, appointment, promotion, remuneration, discipline, termination, admissions, assessment, progression, financial support, or other decisions that may have legal or similarly significant effects on an individual, unless specifically assessed and approved as lawful under POPIA and applicable Institute requirements.
- f. Rely on AI-generated legal, financial, regulatory, cybersecurity, academic or other high-impact advice without competent human review.
- g. Use AI-generated citations, references, statistics, quotations, or factual claims without verification against reliable sources.
- h. Connect autonomous AI agents, bots or integrations to Institute systems, mailboxes, SharePoint sites, databases, or other information repositories without Executive: Technology Management and Department Head approval.

10. DATA PRIVACY AND CONFIDENTIALITY OBLIGATIONS – ALL USERS

Every user, including every Board member and member of staff, has a personal obligation to protect information before it is submitted to an AI system. The following requirements are mandatory:

Obligation	Minimum requirement
Minimise	Use the least amount of information necessary. Remove names, identifiers, and unnecessary detail wherever reasonably possible.
Classify	Determine whether the information is public, internal, confidential, or restricted before using it with AI.

Authorise	Use only an AI service approved for the relevant information classification and business purpose.
Protect	Do not place confidential or restricted information in public AI services or personal AI accounts.
Verify purpose	Personal information may only be used for a lawful, specific, and authorised purpose consistent with POPIA and the reason it was collected.
Check retention and training	Where relevant, confirm whether prompts, files and outputs may be retained, reviewed by the provider, or used to improve/train models. High-risk data may only be used where approved controls prevent inappropriate reuse.
Control sharing	AI-generated outputs containing personal or confidential information may only be shared with authorised recipients.
Review output	Check that AI outputs do not expose, infer, combine, or reproduce personal or confidential information beyond what is necessary.
Record appropriately	Where an AI-assisted output becomes an institutional record, it must be stored and retained in accordance with TM10: Records Management Policy.
Report	Any accidental upload, disclosure, unauthorised access, or suspected compromise involving AI must be reported immediately through the prescribed security/data-breach channels.

10.1 Information handling matrix for AI use

Classification	Examples	AI handling rule
Public	Published website content, approved public brochures, public legislation	Permitted in approved AI services. Public AI may be used where no other restriction applies. Output must still be verified.
Internal	Routine internal process notes, non-sensitive working material	Use approved Institute AI services. Avoid personal accounts where the information is work-related.

Confidential	Non-public strategy, contracts, internal financial information, non-public research, employee/student information	Only in an AI service specifically approved for confidential information and only where the use is necessary and authorised.
Restricted	Special personal information, credentials, highly confidential Board matters, disciplinary/investigation records, privileged legal advice	Do not use with AI unless the specific use case, service and safeguards have received written approval from the appropriate authority, including the IO/DIO and/or Technology Management where applicable.

11. SPECIFIC DATA PRIVACY OBLIGATIONS FOR BOARD MEMBERS

Board members occupy positions of trust and regularly receive information that is highly confidential, personal, commercially sensitive, or legally privileged. Board members are subject to the same minimum requirements as all users and the following additional obligations apply:

- a. Board packs, committee packs, agendas, draft minutes, resolutions, governance evaluations, risk reports, strategic plans, forecasts, remuneration information, investigations, complaints, disciplinary matters, legal advice, and other non-public Board information must not be uploaded to a public AI service or processed through a personal AI account.
- b. A Board member may use AI with Board information only where The Institute has approved the AI service and the particular use is consistent with the information classification, contractual safeguards and POPIA requirements.
- c. Board members must not upload personal information relating to fellow Board members, employees, students, complainants, whistle-blowers, suppliers, or other stakeholders into an unapproved AI service.
- d. Legally privileged or litigation-related information must not be submitted to an AI service unless the use has been authorised and the legal/confidentiality implications have been assessed.
- e. AI may assist with analysis or drafting, but Board members remain responsible for their own judgement, fiduciary duties, deliberations, decisions, and votes. AI must not replace independent Board consideration.
- f. AI-generated summaries of Board papers must be checked against the original source material. A Board member must not rely on an AI summary as the sole basis for a material governance decision.
- g. AI-generated Board papers, resolutions or minutes must be reviewed and approved through the normal governance process. AI output does not constitute an official Board record until formally adopted or approved.
- h. AI recording, transcription or meeting-assistant tools may not join, record, transcribe or summarise Board or Board committee meetings unless prior approval has been

obtained from the Chairperson or authorised governance function and the privacy, security and record-retention requirements have been addressed.

- i. Board members must immediately report any accidental disclosure of Board information or personal information to an AI service to the Information Officer/DIO and Technology Management, regardless of whether the Board member believes harm is likely.

12. STAFF AND MANAGEMENT DATA PRIVACY OBLIGATIONS

All employees, executives, managers, academic staff and other staff users must apply privacy and confidentiality controls throughout the AI lifecycle. In particular:

- a. Managers may not instruct staff to upload personal or confidential information into an AI service that has not been approved for that information.
- b. Employee performance information, recruitment information, disciplinary records, grievances, medical information, payroll information and other People Management records may not be processed through public AI services.
- c. Student applications, identity information, contact details, assessment submissions, marks, academic records, disability information, financial records and support information may not be processed through public AI services.
- d. Where AI is used to support HR, admissions, academic, finance, student-support or other decisions affecting individuals, the responsible staff member must validate the input data, review the output, and retain meaningful human decision-making.
- e. Sensitive prompts and outputs must not be copied into personal email, personal cloud storage, consumer messaging services or other unauthorised locations.
- f. Users must follow any approved retention, deletion and secure-sharing requirements for prompts, uploaded files, and AI-generated records.

13. AI TOOLS, PROCUREMENT AND VENDOR DUE DILIGENCE

AI services used for institutional purposes must be assessed according to risk. Technology Management, together with the Information Officer/DIO and other relevant stakeholders, must consider the following before approving high-risk or enterprise AI services:

- a. The nature and sensitivity of the information to be processed.
- b. Whether the service provider acts as an operator or otherwise processes personal information on behalf of the Institute.
- c. Contractual privacy, confidentiality, and security obligations, including breach notification and sub-processor arrangements.
- d. Whether prompts, files and outputs are retained, used for service improvement, or used to train provider models.
- e. Data location, international transfers and whether cross-border processing is consistent with POPIA requirements.
- f. Identity and access controls, logging, encryption, administrative controls and user management.
- g. Data deletion, export and termination arrangements.
- h. Model limitations, bias, explainability and suitability for the intended use.

- i. Integration permissions and the extent of access to Institute systems, mailboxes, files or datasets.
- j. Vendor support, resilience, incident handling and business continuity.

Procurement and renewal of paid AI services must also comply with TM9: IT Asset and Acquisition Policy and the Delegation of Authority.

14. PROCESSING PERSONAL INFORMATION WITH AI

AI does not create an exemption from POPIA. Where AI processes personal information, The Institute and its users must continue to comply with the applicable conditions for lawful processing. This includes accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.

14.1 Special personal information and high-risk data

Special personal information and other high-risk personal information may only be processed using AI where the processing is lawful, necessary, appropriately authorised and supported by safeguards suitable to the risk. Public AI services must not be used for such information.

14.2 Automated decision-making

AI must not be used as the sole basis for a decision that has legal consequences for a person or substantially affects that person unless the processing is lawful under POPIA, the relevant exception or basis has been confirmed, and appropriate safeguards and human review have been approved. High-impact decisions must remain meaningfully reviewable by an authorised human decision-maker.

14.3 Cross-border processing

Where an AI service processes or stores personal information outside South Africa, the responsible business owner, Technology Management, and the Information Officer/DIO must ensure that the transfer and processing arrangements comply with applicable POPIA requirements before restricted or high-risk personal information is processed.

15. ACCURACY, BIAS AND HUMAN OVERSIGHT

- a. Users must assume that AI can generate inaccurate, incomplete, outdated, biased or fabricated content.
- b. Material AI outputs must be verified against reliable source material before being used for decision-making, formal communication, academic content, policy, legal interpretation, financial reporting or governance purposes.
- c. AI-generated references and citations must be checked against the original publication or authoritative source.
- d. Users must consider whether an AI output may produce unfair discrimination, stereotyping or unjustified profiling.

- e. Where AI contributes materially to a decision affecting a person, the human reviewer must understand enough of the basis and context to exercise genuine independent judgement.

16. INTELLECTUAL PROPERTY, COPYRIGHT AND CONFIDENTIAL KNOW-HOW

- a. Users must respect copyright, licensing, database rights, confidentiality, contractual restrictions, and other intellectual property rights when providing content to AI or using AI-generated content.
- b. Users must not upload third-party confidential information, licensed content, unpublished research, assessment banks, proprietary courseware, or other protected material where the relevant rights or permissions do not allow such processing.
- c. AI-generated content must not be represented as wholly original human work where disclosure is required by academic, professional, or institutional rules.
- d. Users must verify The Institute's ownership, licensing, and reuse rights before commercially publishing, licensing or materially relying on AI-generated content.

17. AI MEETING RECORDING, TRANSCRIPTION AND SUMMARISATION

- a. Users must not enable an AI meeting bot, recorder, transcription service or summarisation tool without considering whether attendees have been appropriately informed and whether the processing is authorised.
- b. Board, Board committee, disciplinary, grievance, legal, executive, or other sensitive meetings require specific prior approval before an AI recording or transcription service is used.
- c. Meeting transcripts and summaries containing personal or confidential information must be stored, shared, and retained according to the applicable information classification and Records Management Policy.
- d. AI-generated minutes are draft support material only. Official minutes must be reviewed and approved through the relevant governance process.

18. SECURITY INCIDENTS, DATA BREACHES AND MISUSE

Any suspected AI-related security incident, misuse or personal-information compromise must be reported immediately. Examples include accidental uploads to the wrong AI service, disclosure of confidential information, unauthorised access to AI accounts, compromised credentials, malicious AI-generated content, unexpected data exposure or an AI integration accessing information beyond its approved scope.

Technology Management must handle information-security aspects in accordance with TM2: Information Security Management and TM4: Incident and Service Management Information Technology. Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the matter must be

escalated immediately to the IO/DIO and handled in accordance with TM6: Data Breach Policy. Users must not delay reporting while attempting to determine whether the incident is serious.

19. ROLES AND RESPONSIBILITIES

Role	Responsibility
The Board	Provides governance oversight and is responsible for using AI in a manner consistent with its governance and fiduciary responsibilities. Board members must comply with the specific privacy and confidentiality requirements in this Policy.
Information Officer / DIO	Provides oversight of POPIA compliance, privacy risks, personal-information processing and security-compromise obligations associated with AI use.
Executive: Technology Management	Custodian of this Policy; oversees AI technology governance, approval, security assessment, access controls, technical risk and integration with the information-security framework.
Executives and Management	Ensure staff under their control understand and comply with the Policy, and that AI use cases are appropriate, authorised, and subject to human oversight.
People Management	Ensures AI use involving employee and recruitment information is aligned with privacy, fairness, and employment requirements.
Academic / Research Management	Ensures AI use in teaching, assessment, research and academic administration complies with academic integrity, research ethics, quality assurance and privacy requirements.
All Users	Protect information, use only authorised AI services, verify outputs, maintain human accountability, and report incidents immediately.
Third-party service providers	Must comply with contractual, confidentiality, security, POPIA and incident-notification requirements applicable to the AI processing performed for the Institute.

20. TRAINING, AWARENESS AND USER ACKNOWLEDGEMENT

- a. The Institute must provide appropriate AI awareness and privacy/security guidance to users based on role and risk.
- b. Board members and staff with access to confidential, restricted, or personal information must be made specifically aware of the prohibition on uploading such information to public or unapproved AI services.
- c. Users may be required to complete AI, privacy or cybersecurity awareness activities and acknowledge this Policy.
- d. Additional role-based training may be required before a user is granted access to high-risk AI systems or integrations

21. MONITORING, RECORDS AND AUDIT

- a. The Institute may monitor approved AI service usage, administrative logs and related system activity where lawful, proportionate and necessary for security, compliance, cost management, audit or investigation.
- b. Records of material AI approvals, risk assessments, vendor assessments, incidents and high-risk use cases must be retained in accordance with TM7: Records Management Policy.
- c. AI-generated content that forms part of an official institutional decision or record must be retained with sufficient context to support accountability and audit where reasonably required.
- d. The Institute may suspend or restrict access to AI services that present unacceptable legal, privacy, security, ethical, operational, or reputational risk.

22. BREACH, NON-COMPLIANCE AND DISCIPLINARY ACTION

Failure to comply with this Policy may expose the Institute, data subjects and other stakeholders to legal, regulatory, financial, security and reputational harm. Non-compliance may result in restriction or removal of AI access, investigation, disciplinary action, contractual remedies, recovery of losses where lawful, and/or referral for civil or criminal action where appropriate.

A user who becomes aware of their own accidental breach must report it immediately. Prompt self-reporting supports containment and does not remove the Institute's obligation to investigate the incident appropriately.

23. REVIEW OF THIS POLICY

Regular review and amendment of this Policy will be undertaken in line with approved institutional policy governance and regulatory requirements. The Policy must also be

reviewed where material changes occur in applicable law, AI technology, institutional risk, approved AI services or national AI governance requirements. The official custodian is the Executive: Technology Management, with the Information Officer consulted on material privacy and personal-information provisions.