INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Policy Code: TM12
Version: 3
Approved by: The Board
Approval Date: 11/04/2024
Decision No.: B.01.2024.02

The Da Vinci Institute for Technology Management (Pty) Ltd
Registered with the Department of Education as a private higher education institution under the Higher Education Act, 1997. Registration Certificate No. 2004/HE07/003

Table of Contents

1. Introduction

The Da Vinci Institute is a private higher distance education institution offering programmes with outcomes-based curricula. This policy forms part of the institutional 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 Mode 2 discourse on the generation and distribution of knowledge.

This policy forms part of the set of quality management policies of The Da Vinci Institute for Technology Management.

Da Vinci offers outcomes based, distance education opportunities. The policies and procedures detail the principles and processes that will ensure that learning programme offerings are aligned to the principles of a Mode 2 higher education institution, whilst adhering to the required academic standards and empowering students with the knowledge, skills and values to contribute to their communities, society and economy of the future.

2. Definitions

Term	Definition
Workstation	A computer used to complete work. The term workstation may refer to a desktop model of computer or a laptop model of computer.
Information Technology	The branch of engineering that deals with the use of computers and telecommunications to retrieve and store and transmit information
Information Technology Department	The campus Information Technology staff consisting of the ICT Manager, System Administrator, IT Specialists and IT support staff

3. Legislative compliance

This policy is benchmarked against and should be read in the context of the relevant legislation underpinning the principles against which institutional policies and operational procedures are developed, implemented and maintained. These include:

- Constitution of the Republic of South Africa: 1996
- Higher Education Act (Act 101 of 1997)
- NQF Act, No. 67 of 2008

- SAQA - National Policy and Criteria for Designing and Implementing Assessment for NQF Qualifications and Part-Qualifications and Professional Designations in South Africa
- CHE: Higher Education Quality Committee (HEQC) Criteria for Programme Accreditation: November 2004
- Labour Relations Act (Act 66 of 1995) as amended.
- CHE: Distance Higher Education Programmes in a Digital Era: Good Practice Guide

4. SCOPE

The intended recipients of this policy are all internal departments within the Da Vinci Institute.

5. PURPOSE

Da Vinci's entire ICT represents a critical operational resource of significant capital outlay. It is therefore of utmost importance to ensure that Da Vinci's ICT is properly managed, administrated and protected.

The purpose of this policy is therefore not only to prevent abuse of Da Vinci's ICT resources and reduce the risk of errors, fraud and the loss of data, confidentiality, integrity and availability, but to ensure that the ICT is optimally used and applied to the best advantage of DaVinci in meeting its strategic objectives.

6. ICT ACCESS CONTROL & SECURITY

6.1. General:

- A user's access to ICT is a privilege not a right, and must be treated as such by all users;

- A user's ability to access ICT does not, in itself, imply authorization to do so, and hence users must ascertain what authorizations are to be obtained for access and must obtain such authorization before proceeding to access any ICT.

6.2. Username and Password Control

- Usernames and passwords are an important aspect of ICT access control and security and serves as the front-line protection for ICT

- Poorly selected and maintained passwords may result in the compromise of Da Vinci's ICT and as such users are personally responsible for taking the

appropriate steps to safeguard their username and passwords since a user will be personally responsible for any transaction/activity that is made with his / her username and password where it is found that they acted negligently in the securing and/or protection of their username or password

- Users shall adhere to the specifications for usernames and passwords as communicated by the ICT Manager, from time to time. It is a user's personal responsibility to ensure that their username and password conforms to the latest requirements for ICT.

- A user may not:

    - insert their own, or another user's, username and/or password into an email message or other forms or documents distributed through ICT;
    - use the same password to access all the user's ICT accounts;
    - share, or otherwise reveal, usernames or passwords with other users, including administrative assistants, secretaries, supervisors or managers;
    - leave their workstation unattended without locking their desktop (securing their laptop/pc with a password-protected screensaver);
    - attempt to intercept, redirect or otherwise interfere with or access another user's ICT;
    - store or record usernames or passwords in a manner which may be reasonably accessible to any person.

- The ICT Manager may authorize the release of a username and/or password to a nominated user.

- A user shall immediately notify the ICT Manager if the user suspects that his/her username and/or password has been compromised in any manner whatsoever. Failure to notify the ICT Manager, as set out herein shall be deemed an instance of serious misconduct on the part of the user concerned.

- A user shall immediately cease to have access to any and all user accounts at the moment of suspension or termination of employment, on the last day of employment in the case of resignation, or in such other instance as the ICT Manager may determine from time to time.

6.3. Data Transfer

- Users shall take all reasonable steps to protect and restrict the transfer of confidential or sensitive data (Da Vinci's proprietary or confidential information) from loss, theft or otherwise unauthorized access thereto by other users and

third parties, to avoid reputation and pecuniary damages to DaVinci.

- Da Vinci's proprietary or confidential data / information may only be transferred between users and authorized third parties or copied to other media (storage devices), when the integrity and security of the data can be assured, and all such data / information should be encrypted when transferred / transmitted. All transfers / transmissions of data / information, using whatsoever component of ICT, must be duly authorized prior to the transfer or transmission.

7. ICT INTEGRITY

7.1. Viruses & other forms of malicious software:

- Viruses and other forms of malicious software (worms, trojans, backdoors, VBS scripts, mass-mailers, spyware etc.) represent a significant threat to ICT. Viruses and other forms of malicious software are programs designed to make unauthorised changes to ICT and can compromise ICT integrity by, for example, allowing information to be transmitted outside da Vinci, damaging data, facilitating unauthorised access to ICT etc.

- To protect ICT integrity users may not:

  - use untrusted sources for data and software acquisition, downloading or installation;
  - open any attachments or click on any link to an email from an unknown, suspicious or untrustworthy source;
  - download files from unknown or suspicious sources including, but not limited to, the internet, Universal Serial Bus (USB flash drives), Secure-Digital Cards (SD Card) or any other form of removable media for data storage;
  - engage in direct disk sharing with read / write access, unless there is a business requirement to do so;
  - modify, change, deactivate, or otherwise tamper with existing anti-virus / protection software.

7.2. Remote Access

- Users who are granted access to the cloud-based systems and services must remain constantly aware that these connections provide direct access to da Vinci's most sensitive operational/confidential information. As such, cloud

access serves as an extension of da Vinci's ICT infrastructure, and users must exercise utmost caution in their interactions with the cloud environment.

- Only authorised users may access cloud-based systems and services, and it is the responsibility of users with cloud access privileges to ensure that their access credentials are not shared with third parties or misused in any way.

- Cloud access will only be granted to users who have a valid business need, and access permissions will be periodically reviewed and monitored to maintain proper authorisation levels and compliance with da Vinci's security policies.

7.3. ICT Standards

- DaVinci has determined, and will from time to time re-determine, standards for all ICT and no user may use any ICT in connection with da Vinci's business or in execution of their duties, or otherwise, that is not part of the determined ICT standards without the necessary approval of the ICT Manager

- No user is allowed to "plug" any equipment into, or install any software onto, the ICT device without prior approval from the ICT Manager. Should a user wish to deploy any equipment, or install any software, that is not part of da Vinci standards, the request with proper motivation must be forwarded to the ICT Manager for consideration

- DaVinci is allowed to disconnect and/or remove any unauthorized equipment or software from the ICT device and shall not be liable to the user for any damage or loss, direct or otherwise, caused by such disconnection and/or removal

- Users are required to properly protect and maintain ICT devices, and specifically hardware and peripherals, and in this regard users:

    - should take care when consuming beverages near their ICT devices;
    - may not consume food near their ICT devices;
    - may not smoke near their ICT devices, including at home;
    - may not attempt to clean their ICT devices themselves, but should in the case of spillage, immediately dry the spillage with a paper-towel and inform the IT Service Desk in accordance with section 11 below. The IT Service Desk shall be responsible for cleaning ICT devices, as and when necessary;

- may not dismantle, open or otherwise modify any ICT device or a component thereof.

- The procurement and disposal (buy, sell, rent, lend or otherwise acquire or dispose) of ICT devices shall be the responsibility of the ICT Manager and a request, together with a motivation therefore, for the procurement or disposal of ICT shall be done in accordance with the provisions of section 11 below.

7.4. Back-ups & File Management

- All users shall ensure that data related to their work duties is properly stored, organized, and backed up in their assigned OneDrive account and relevant SharePoint locations to ensure da Vinci's data integrity and security.

- Users will be responsible and must maintain data OneDrive synchronization between their local devices and OneDrive to facilitate effective backup and data accessibility.

7.5. Mobile Devices

- Mobile Devices such as smartphones, tablets, and the like enable remote ICT connectivity and therefore create additional security concerns for da Vinci. Mobile Devices are not considered secure devices

- Only authorized users may synchronize their e-mails and calendar accounts to their Mobile Devices, but may under no circumstances store proprietary or confidential data / information on the device (including data / information contained in e-mails), due to the high risk of theft or loss of mobile devices

- Users shall ensure that their Mobile Devices are, in the very least, password protected and shall take reasonable steps to prevent the theft or loss of their device(s)

- Mobile Devices not owned by da Vinci may not be connected, either directly or indirectly, to the ICT infrastructure without the knowledge and authorization of the ICT Manager.

8. E-MAIL, INTERNET AND SOCIAL MEDIA:

7.1 General:

The directives in this section 3 are intended to protect da Vinci from potential legal liabilities should a user contravene the laws of the Republic of South Africa when using email, social media platforms or internet, and to protect propriety and/or confidential business information of da Vinci from unauthorized access and / or disclosure to third parties and to safeguard the reputation, dignity and privacy of da Vinci and users alike.

7.2 Content of E-mails

- The da Vinci Institute takes a zero-tolerance approach to instances of unacceptable behavior relating to the distribution of e-mails. Unacceptable behaviour includes, but is not limited to; distributing (sending or forwarding) e-mails outside the scope of the user's employment duties with da Vinci that:

    - directly or indirectly promotes / supports, or purports to promote / support specific racial, sexual, cultural or religious views, ideas or opinions;
    - contains, or purports to contain, political propaganda, undertones or nuances;
    - contains, or purports to contain, content promoting any type of discrimination or harassment;
    - contain, or purports to contain, obscene, offensive, profane, derogatory or defamatory images or words;
    - contain chain letters, petitions, junk mail or hoax messages;
    - contains unsolicited or unauthorized mass e-mail (spam), including messages relating to other users' health, wellbeing, achievements or the like;
    - contains offers of goods and/or services (other than legitimate and authorized da Vinci business) or contains external commercial or personal solicitation content aimed at personal gain (economic or otherwise) for the user or another party;
    - infringes the privacy rights of others;
    - violates any national or international law, infringes on another's intellectual property or commits da Vinci to unauthorized business, policy or costs of whatsoever nature;
    - directly or indirectly releases da Vinci's confidential or proprietary information or causes such information to be released.

9. PRINTERS, COPIERS AND SCANNERS

- Printers, copiers and scanners, or a combination of these, form an integral operational support function to Da Vinci's business and as such they are to be used, protected and maintained accordingly.
- Users shall in making use of printers, copiers and scanners, or a combination of these, adhere to the following directives:
  - Printing and/or copying of non-work-related documents is limited to 10 (ten) double sided A4 pages per user per month;
  - Colour printing is not permitted, unless specifically authorized;
  - Users shall take care not to damage printers, copiers and scanners, or any component thereof, whilst attending to a malfunction (paper jam) or paper / toner replacement;
  - Paper may not be removed from printers and copiers and only standard paper may be used in printers and copiers;
  - Users may not move a printer, scanner or copier from its existing location; under any circumstances;
  - User may not modify, or attempt to modify any printer, copier or scanner, or any component thereof, except for resolving a simple malfunction (paper jam) or changing toner, or changing normal printing, scanning and copying settings for a specific print/copy job. Where users are unsure of the correct process to be followed for removing a paper jam, replacing toner or to change settings, such user must log a request with the IT Service Desk for assistance;
  - User shall report/log a fault or any other cause that prevents the user from printing, scanning or copying to the IT Service Desk, as set out in section 11 below.
  - The procurement and disposal of printers, copiers and scanners shall be dealt with in accordance with section 2.3(e) above.

10. USER DECLARATION AND OBSERVANCE

- All users will be required to confirm their acknowledgement, understanding and acceptance of the provisions of this policy.
- Any users found to have ignored, contravened or otherwise breached the provisions of this policy, may be subject to disciplinary action, up to and including termination of employment, in terms of the Code of Ethics and Disciplinary Regulations, as determined from time to time.

11. ICT SERVICE MANAGEMENT & REPORTING

- Users shall make use of the ICT problem reporting channels (commonly known as the IT Service Desk) as determined from time to time.
- Problems reported to/logged with the IT Service Desk will be resolved as per the priority matrix, as determined from time to time.
- Service requests, of whatsoever nature, not reported or logged with the IT Service Desk shall not be attended to, save to the extent that the IT Service Desk was not accessible/available at the time of reporting/logging, in which case such service request shall be reported/logged manually and later updated when the IT Service Desk becomes available/accessible.

12. 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 Executive Dean.

13. Revision History

Version No.	Amendment Details	Approval date	Approving Committee	Chairperson Signature
Version 1 (V1)	Various	05/10/2015	EXCO	
Version 1a (V1a)	Various	30/07/2018	EXCO	
Version 2 (V2)	1. Included definition of ICT Manager, on the definitions table. 2. Included "additional information(or click on any URL Link)", under ICT integrity. 3. Included a comment in Point 7.2 I Indicate Cloud access, not VPN Access as the remote medium. 4. Amended point 7.4 to OneDrive Backups.	13/09/2023	EXCO	

V3	Amendments as per review tracking document: Amendment review	11/04/2024	The Board	

USER SET-UP PROCEDURE

14. Procedure Description

This procedure document will be used by the Information Technology Office when setting up a new user or updating a user.

Step	Description	Notes
1	Information Technology (IT) Office to receive new user/update of user form from Human Resource Department with all requirements for individual	
2	Either old machine is restored and formatted, or new machine is purchased	
3	IT Office to ensure that the machine is loaded with the relevant software	
4	New User: IT Office to ensure that the user is loaded, user profile created, and e-mail account set up and access control to the public folder is set	
5	IT Office to update the asset register	
6	IT Office hand the machine over to the individual or set it up at the individual's desk	
7	Employee to sign for machine	
8	IT Office to ensure that all devices are updated and maintained on a regular basis	Software updates are automatic

Stakeholders

#	Stakeholder
1	Executive: Operations
2	IT Office

Version History

Policy Code	C10-P1	Authorised by	Benjamin Anderson
Version	V1	Signature	
Date Approved	01/07/2018		