ACCEPTABLE USE OF INFORMATION SYSTEMS POLICY

Policy Code: TM1
Version: 3
Approved by: The Board
Approval Date: 11/04/2024
Decision No.: B.01.2024.01

Table of Contents

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-based Action Learning discourse on the co-creation and distribution of relevant knowledge.

Access to computer systems and networks owned, and or operated by The Institute, imposes certain responsibilities and obligations, and is granted subject to The Institute's policies and procedures. Acceptable use should always be done ethically, reflect honesty and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and the individuals' right to privacy.

Information technology offers increased opportunities for communication and collaboration in the way The Institute conducts business as an institution by providing the following services:

- Email
- Wireless connectivity
- Internet access
- Voice over Internet Protocol (VoIP)
- Video Conferencing, for example, Zoom, MS Teams, etc.

These resources require responsible utilisation of every user.

The Institute's information resources consist of its computer devices, data, applications, and the supporting network infrastructure. These technologies are critical to the undertaking of The Institute to provide quality access to users and quality education to its students utilising The Institute's information systems. Electronic communications should meet the same standards for distribution or display as for paper documents.

Users are expected to comply with all applicable legislation. The Institute reserves the right to terminate information system services of users who repeatedly violate the rules or infringe upon the rights of copyright holders.

2. DEFINITIONS

Term	Definition
Communication	The imparting or exchanging of information by speaking, writing, or using some other medium
Discriminatory	Offensive, untrue or provocative material based on race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, belief, culture, language and birth
Equipment	Includes computers, desktops, servers, routers, laptops, telephones, networks, cell phones, electronic handheld devices, mobile devices/tablets, facsimile machines, pagers, software, hardware and/or similar equipment owned by, licensed to, or rented by The Institute, or user equipment that is utilised during business hours at The Institute
Illegal Content	Material that is pornographic, discriminatory, oppressive, racist, hate speech, sexist, defamatory against any user or third party, offensive to any user or group, a violation of a user's or a third party's privacy, identity or personality, copyright infringement, trade mark infringement, religious or political beliefs, malicious codes such as viruses, spyware and malware, cartoons, jokes and content containing any personal information of third parties without their express consent, and includes hyperlinks or other directions to such content
Intercept	To filter, scan, block, redirect, access, disrupt, copy, print, disclose, retain, use, collect, delete and/or record, in any format and in any manner
Internet	A set of computer networks that utilise the internet protocol (IP) and shall in all cases include The Institute's intranet, mobile networks or wireless access areas or local access networks
Monitor	To listen to, or record communications by means of a monitoring device
Personal Information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person (b) information relating to the education or the medical, financial, criminal or employment history of the person (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person

Term	Definition
	(d) the biometric information of the person (e) the personal opinions, views or preferences of the person (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence (g) the views or opinions of another individual about the person (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
Pornographic Content	All the content and actions, simulated or real, graphic or written, detailed in the Films and Publications Act 65 of 1996
Record	Any content, document, record, file, data, information, picture, download, graphic, depiction, representation or software that is created, used, accessed, disclosed, copied, stored, received or delivered by a user, regardless of the format thereof
User	All persons, including, but not limited to employees (permanently or temporary), directors, consultants, contractors and students who have access to, or the use of The Institute's equipment and communication system
VoIP (voice over IP)	Is the transmission of voice and multimedia content over Internet Protocol (IP) networks. VoIP is enabled by a group of technologies and methodologies used to deliver voice communications over the internet, enterprise local area networks or wide area networks
Video Conferencing	Video conferencing is a technology that allows users in different locations to hold face-to-face meetings without having to move to a single location together

3. REGULATORY FRAMEWORK

This 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. Constitution of the Republic of South Africa (No.108 of 1996)
   ii. Electronic Communications and Transactions Act (No.25 of 2002)
   iii. Films and Publications Act (No.65 of 1996)
   iv. Promotion of Access to Information Act (No.2 of 2000)
   v. Protection of Personal Information Act (No.4 of 2013)

I. A4 - Privacy and Confidentiality Policy
II. A7 – Communications Policy
III. B25 – Social Media Policy
IV. C1 - Electronic Information and Communication System Policy
V. C3 - Information Security Management Policy
VI. C4 – Firewall Policy
VII. C5 - Wireless Communication Policy
VIII. C6 - Change Management Information Technology Policy
IX. C7 - Incident and Service Management Information Technology Policy
X. C8 - Disaster Recovery Information Technology Policy
XI. C9 – Backup Policy
XII. C11 - Data Breach Policy

4. SCOPE

This Policy applies to students, faculty, staff and other stakeholders of The Institute utilising The Institute's information systems resources.

5. PURPOSE

a) The purpose of this Policy is to outline the required governance for users utilising The Institute's information systems.
b) The requirements of this Policy apply to personal as well as business communications:
    I. These communications can result in binding obligations and expose The Institute to liability in the same way as conventional correspondence.
    II. Improper statements communicated could cause personal liability for the individual sending it, as well as being disclosed in court and the court proceedings. The same protocols and standards apply to electronic communications as for written correspondence.

6. PRIVACY

a) Electronic communications transmitted across a network is not considered private or confidential as the email can be retrieved from the central server or by making use of specialist software.
b) Information Technology (IT) administrators may become aware of unacceptable or problematic file content while dealing with specific operational problems. Usage logs are kept to diagnose such problems. Cloud storage usage logs are kept for a standard period as per Microsoft standard operating procedures as well what the Microsoft subscription license allows.

c) The Institute will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance includes providing, when required, copies of system files, email content, or other information ordered by the court.

d) The Institute does not monitor personal internet web pages for the purpose of determining content. When credible evidence of illegal or otherwise impermissible activity is reported, appropriate action will be taken.

e) IT administrators may become aware of activity that poses a risk to the network's proper operation. In such cases, IT administrators may need to disable or block access to the services or systems involved if they are deemed to pose a risk to the network's optimal performance.

f) During the process of diagnosing potential problems involving the proper function of the network, any information obtained that indicates possible unauthorised distribution of copyrighted materials will be referred to the Head of Information and Communication Technology for further investigation.

7. RESPONSIBILITIES OF USERS

a) Access to The Institute's electronic communications services is a privilege, and certain responsibilities accompany this privilege. People who make use of The Institute's communication services such as email, the Internet and telephone systems are expected to use this service in an ethical and responsible manner.

b) In the event of non-compliance to this Policy, certain violations may be treated as gross misconduct and could result in disciplinary action including summary dismissal in accordance with The Institute's disciplinary procedure

c) All users are expected to protect The Institute's information resources by preventing access to their computers, or to the access port assigned for the employee's exclusive use, from unauthorised electronic access by using effective passwords and by safeguarding those passwords.

d) Data stored on The Institute's computer system may provide an access point for the entire computer system if the users' computer is not password protected.

e) Users have to identify themselves clearly and accurately in all electronic communications. Concealing or misrepresenting a name or affiliation to dissociate oneself from responsibility could result in disciplinary action.

f) All stored electronic correspondence should be assumed to be private and confidential unless the owner has granted permission to make it available to others.

g) Users are expected to promote efficient use of network resources, consistent with the instructional, research, public service, and administrative goals of The Institute.

h) Users have to show consideration for others and refrain from engaging in any use that would interfere with the work of others or disrupt the intended use of network resources.

i) Users will be held responsible for destructive or illegal activity done by someone to whom they allowed access, even if the computing resource does not require a password.

j) Civil dialogue at The Institute is conventional, free of intimidation and harassment. It is based upon respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable, it is the user's responsibility to do so in a way that advances the cause of learning and mutual understanding.

k) Users may not accept payment, or otherwise profit from the use of any company-provided information resources, or from any output produced using it.

l) Users may not promote any commercial activity using company information resources. Examples include, attempting to sell event tickets or advertising a 'Make Money Fast' scheme via a newsgroup. Such promotions are considered unsolicited commercial spam and may be illegal as well.

m) Users may never use any company-provided information resource to act in a manner that is illegal, threatening, or deliberately destructive, not even as a joke. Violations can result in disciplinary action, criminal charges, or both.

n) Users may not deliberately install unauthorised or malicious software on any system. Violations can result in disciplinary action, criminal charges, or both.

o) Users may not send rude or harassing correspondence. If someone requests a user to stop communicating with him or her, the user should do so. If the user fails to do so, the person can file a complaint and the user can be disciplined.

p) Users should not interfere with the activities of others or use a disproportionate share of information resources.

q) Users should not send an unsolicited message(s) to a large number of recipients, known as 'spamming ', the network.

r) Users should never falsify their identity or enable others to falsify their identity using The Institute's information resources. This type of falsification can result in serious criminal penalties and disciplinary action.

s) All electronic correspondence must correctly identify the sender.

t) All electronic correspondence belongs to the originator and should be treated as private communication unless the author has overtly made it available to others.

u) Users may not infringe upon someone else's copyright. It is a violation of company policy and government law to participate in copyright infringement.

v) Users may not try to circumvent login procedures on any computer system or otherwise attempt to gain access where the user is not allowed.

w) Users may not deliberately scan or probe any information resource without prior authorisation. Such activities could result in serious consequences, including disciplinary action.

x) Users may not disclose confidential or restricted data without appropriate authorisation. Business data may be classified as confidential or restricted data,

such as the status of negotiations, terms of contracts, and new research or products, or commercial relationships under development.

y) Users must ensure that any individual with whom the user shares confidential or restricted data is duly authorised to receive this information.

z) Users may not share confidential or restricted data with friends or family members.

aa) Users must comply with The Institute's agreements to protect vendor information such as proprietary methodologies and contract pricing.

bb) Users must report violations of company policies regarding use and/or disclosure of confidential or restricted information to the Head of Information and Communication Technology.

cc) Reading, recording, copying or listening to messages and information delivered to another person's system, without prior permission is prohibited.

8. EMAIL AND INSTANT MESSAGING

a) Emails are permanent and will be available for future reference, as may be some instant messages. All messages shall be treated as potentially retrievable, either from the main server or using specialist software.

b) The email and instant messaging systems exist for business communication and shall not be used to engage in conduct contrary to The Institute's ethics. Whilst personal use is permissible, it must be kept to a minimum, and not interfere with the proper performance of duties or prevent a business activity taking place, or delay, or take precedence over normal business activities.

c) Copies of emails should be stored in accordance with The Institute's requirements and procedures, e.g. in specific archiving folders, or on a shared drive.

d) Users should not communicate anything in electronic format that could jeopardise the integrity or reputation of The Institute, or which the user cannot or would not be prepared to justify.

e) Highly confidential or monetary-sensitive information should not be sent within the main text of an email but should be sent in the form of either a password-protected attachment, encrypted attachment, or as a separate attachment.

f) In the event that the user is of the opinion that they have been harassed or bullied or offended by material sent to them by a colleague via electronic communication, they should inform the head of their department.

9. CATEGORIES OF PROHIBITED ELECTRONIC COMMUNICATION

a) Material which breaches the user's obligations of confidentiality to The Institute, or The Institute's obligations of confidentiality to any client or third party, or is in breach of the proprietary interest, trademark, trade secret or copyright of others will result in disciplinary action being taken due to violation of the requirements of this Policy.

b) Users must not use the electronic communication systems to compose, store, send, receive, forward or otherwise transmit any material in any of the categories noted below. This may constitute misconduct and could result in disciplinary action including summary dismissal.

c) Prohibited electronic communication include the following actions:

i. The use of web-based -mail services such as Gmail, Hotmail or Yahoo to send or receive The Institute's business email;
ii. Large personal attachments including screensavers, games, pictures, executable files, video games and/or presentations;
iii. Screensavers, chain letters or notes, junk mail and 'for profit' messages;
iv. Defamatory material;
v. Abusive, offensive, vulgar or obscene material including any type of pornography;
vi. Any material which is untrue or malicious, whether about another member of staff or someone outside The Institute;
vii. Any racist or sexist material;
viii. Any material that could constitute bullying or harassment on the grounds of sex, including sexual orientation, race or disability, or any other form of discrimination;
ix. Any material that could be considered illegal.

10. INTERNET USE AND DATA TRANSFER

a) The procedures and requirements for email use apply equally to Internet practices and data transfers.

b) The user of the internet must ensure that the source of the data or information is reliable and obtain the required verification if necessary.

c) Users must ensure that, in obtaining information or material from websites or from any other source, that the user is not infringing copyright or incurring unauthorised expense to The Institute.

d) Users are responsible for ensuring compliance with any terms and conditions governing the use of external websites, including, but not limited to the terms of use of any instant messaging service.

e) Access to certain sites may be blocked by IT Management. If the user has a legitimate business requirement to be able to access such sites, this request may be submitted to their immediate manager who will escalate the request to IT Management for authorisation.

f) The user shall not visit sites, download material, transfer data or images, store data or images, transmit information, or display web pages that may resort under one of the following (non-exhaustive) categories (allocated the widest meaning of the terms):

I. Defamatory material;
II. Offensive, vulgar or obscene material (including any type of pornography);

III. Any racist or sexist material;
IV. Any material that could constitute bullying or harassment, such as on the grounds of sex, including sexual orientation, race or disability;
V. Any material that could be otherwise considered illegal;
VI. Under no circumstances shall The Institute's IT systems be used to participate in any internet chat room, post messages on any internet message board, or set up or log text on a blog, even in the user's personal time.

g) The Institute's IT systems shall not be used to participate in any form of online gambling.

h) The Institute reserves the right to monitor internet traffic data (including domain names of websites visited, duration of visits, details of any blocked sites visited, and details of files downloaded from the internet) at a network level (covering both personal and business use) in accordance with this policy. The effect of such monitoring may be to reveal certain sensitive personal data about the user. For example, a visit to a website relating to a political party or a religious group may indicate the users' political or religious beliefs. By accessing websites of this type using The Institute's IT systems, users are consenting to The Institute processing any sensitive personal data that may be revealed by monitoring. Users who wish to preserve their personal privacy should not make use of The Institute's IT systems to access any such websites.

11. BREACHES OF 'ETIQUETTE'

a) Disagreements between people, including heated arguments, unless threatening or otherwise unlawful, are not considered violations of this policy.

b) The Institute expects all its users to be polite and courteous.

c) The user may run the risk of violating criminal laws or inviting an action in civil court by posting on email, blogs, and social networks, an angry response that crosses the line beyond merely being rude or stating an unpopular, offensive view.

12. REPORTING AN INCIDENT OF IT MISUSE OR ABUSE

a) Reporting an incident involving the misuse or abuse of IT resources depends upon the nature of the incident.

b) Reporting 'spam' or unsolicited mail, requires the recipient to either notify the Internet service provider (ISP) from which the mail was sent, or report the incident to the IT department.

c) Users who received unwanted communication should report the incident to their immediate manager who will escalate the incident to the IT department.

13. DISCIPLINARY ACTION

a) Disciplinary action for breaches of this Policy include, but are not limited to:
   i. Verbal warnings;
   ii. Written warnings;
   iii. Cancellation of access privileges;
   iv. Disciplinary probation;
   v. Suspension;
   vi. Criminal prosecution.

b) Should user activity violate the law, users could be prosecuted. Should the user not be charged criminally, they can still be suspended from the company.

c) The Institute reserves the right to protect its electronic resources from threats of immediate damage. This may include activities such as disconnecting an offending computer system from the company network, terminating a running job on a computer system, or taking other appropriate action as deemed appropriate.

d) If users are unsure whether an action they are considering is an acceptable use of electronic resources, they have to obtain confirmation from the Head of Information and Communication Technology for approval.

e) Before users report what they believe is an incident of misuse, they have to confirm the incident with their immediate manager.

f) In general, expressions of opinion by members of The Institute are considered as 'free speech' although the opinions expressed may be unpopular or offensive to some, and is not considered breach of this Policy.

g) 'Spam', unsolicited and unwanted email, and other junk mail from a source outside The Institute will be blocked by The Institute's firewall. Should the user still receive spam email, the user should delete the junk mail. Responsibly-administered mailing lists will remove the user's name from their subscriber list if they are requested to do so.

h) Repeated incidents involving offensive email may become harassment. If the user is of the opinion that it is occurring, the user has to report the matter to his/her direct manager or the Head of Information and Communication Technology.

14. REVIEW OF THIS POLICY

Regular review and amendments of this policy will be done in line with the approved institutional policies. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodians of this policy, namely the Information Technology Manager.

15. REVISION HISTORY

Version No.	Amendment Details	Approval date	Approving Committee	Chairperson Signature
Version 1 (V1)	Various	20/07/2021	EXCO	
Version 2 (V2)	Amendments as per review tracking document: Amendment review	11/04/2024	The Board	