ELECTRONIC INFORMATION AND COMMUNICATION SYSTEM POLICY

Policy Code: TM11
Version: 1
Approved by: EXCO
Approval Date: 29/09/2021
Decision No.: EXCO42/2021

Date Reviewed	Version History
06/09/2021	V1

1. INTRODUCTION 3
2. DEFINITIONS 3
3. REGULATORY FRAMEWORK 5
4. SCOPE 6
5. PURPOSE 6
6. POLICY STATEMENT 6
7. COMMUNICATION SYSTEMS 6
8. RESPONSIBILITIES AND DUTIES 7
9. ACCEPTABLE USE OF SYSTEMS AND EQUIPMENT 8
10. UNACCEPTABLE USE OF SYSTEMS AND EQUIPMENT 9
11. EQUIPMENT AND DATA SECURITY 11
12. WORKING REMOTELY (OFF-SITE) 12
13. RIGHT TO MONITOR, INTERCEPT AND EXAMINE COMMUNICATION 13
14. RIGHT TO SEARCH 15
15. EMAIL SIGNATURES 15
16. EMAIL LEGAL NOTICE 15
17. EMAIL FOR ADVERTISING/NEWSLETTER PURPOSES 16
18. DUTY TO DISCLOSE AND REPORT BREACH OF PROVISIONS 16
19. CONSEQUENCES OF MISCONDUCT 16
20. POLICY CHANGES 17
21. REVIEW OF THIS POLICY 17

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 Institute's 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 Electronic Information and Communication System policy articulates The Institute's vision, strategy, and principles as they relate to the management and use of information and information technology resources, while supporting core academic teaching and learning initiatives. This policy stipulates compliance with applicable laws and regulations, promotes operational efficiency, and manages institutional risk by specifying requirements and standards for the consistent management of information technology resources across the institution.

Communications include:

a) Oral and verbal utterances of a user in or during a meeting where the business of The Institute or related matters are discussed
b) The transfer of any information whether speech, data, text, signals, radio frequency spectrum, or images in any format through communications
c) Access to, or use of the services available on the Internet, including email, instant messaging, websites, file transfer, video conferencing, Voice-over Internet Protocol (VoIP), chat rooms and bulletin boards by users.

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	Include 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 are 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,

Term	Definition
	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 and 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 (P) 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
Monitoring Device	Any electronic, mechanical or other instrument device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to, or record any communication
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 (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

Term	Definition
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
Removable Media	Any data storage unit that can be removed from the equipment and Da Vinci's premises, and include, but is not limited to Flash Cards, Flash Disks (memory sticks), Tapes; Drives, CD's, CD Writers, DVD's and DVD writers
USB (Universal Serial Bus)	Is a common interface that enables communication between devices and a host controller such as a personal computer. It connects peripheral devices such as digital cameras, mice, keyboards, printers, scanners, media devices, external hard drives and flash drives
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

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 and 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. Films and Publications Act (No.65 of 1996)
   v. Promotion of Access to Information Act (No.2 of 2000)
   vi. Protection of Personal Information Act (No.4 of 2013)

B. Applicable Da Vinci documents:
   i. A4 – Privacy and Confidentiality Policy
   ii. A12 – Records Management Policy
   iii. B25 – Social Media Policy
   iv. C2 - Acceptable Use of Information Technology Systems Policy
   v. C3 - Information Security Management Policy
   vi. C4 - Firewall Policy
   vii. C5 - Wireless Communication Policy
   viii. C7 – Incident and Service Management Policy
   ix. C8 - Disaster Recovery Information Technology Policy
   x. C9 - Backup Policy

xi. C10-Information and Communication Technology Policy

4. SCOPE

This policy applies to all users who have access to, as well as third parties who have temporary access to, and/or use of The Institute's communication systems or equipment, including, but not limited to all staff, students, contractors, visitors and vendors.

5. PURPOSE

The purpose of this policy is to:

a) Inform and educate users on the access to, and use of communication systems and equipment
b) Create rules for the access to, and use of The Institute's communication systems and equipment
c) Provide for the interception of communications
d) Provide for disciplinary action against users who fail to comply with this policy
e) Ensure and maintain the value and integrity of The Institute's equipment and network(s).

6. POLICY STATEMENT

The Institute's communication systems and equipment are intended to promote effective communication and working practices within The Institute and are critical to the success of its business. This policy outlines the standards required by users of these systems to notice the circumstances in which The Institute will monitor use of these systems, and the action that will be taken in respect of breaches of these standards.

Users must use The Institute's communication systems and equipment sensibly, professionally, lawfully, consistently with the user's duties, with respect for his/her colleagues, and in accordance with this policy and The Institute's other policies, rules and procedures.

All information relating to The Institute's clients/customers and its business operations is confidential. Users must treat The Institute's paper-based and electronic information with utmost care.

7. COMMUNICATION SYSTEMS

a) The facilities made available or allowed by The Institute for business purposes which include, but not limited to Internet access, email access and use of any equipment for purposes of:
   I. Accessing, creating, copying, distributing, sharing and deleting records.
   II. Initiating, creating, receiving or storing communications.

b) The Institute owns the legal right and duty to:

I. Regulate all use of its equipment and communication system
II. Secure and maintain its equipment and communication facilities
III. Ensure the confidentiality of its intellectual property, trade secrets, client information, employee information and confidential information
IV. Protect the privacy of its clients
V. Identify and address the potential risks associated with the use of equipment and communication systems in the workplace
VI. Promote employee productivity
VII. Comply with the provisions of laws and regulations that govern the access, use and interception of communications
VIII. Investigate and prosecute illegal or unauthorised use of its communication and/or equipment
IX. Respect and protect every employee's right to privacy, free speech, and the right to receive and impart with information as detailed, amongst others, in the South African Constitution of 1996.

c) To successfully execute The Institute's obligations, The Institute needs to:

I. Monitor and intercept employee communications
II. Secure and maintain the equipment and communication systems as detailed in this Electronic Information and Communication System Policy.

8. RESPONSIBILITIES AND DUTIES

All users are responsible for the success of this policy and should ensure that they have read and are familiar with the content. Any misuse of The Institute's communication system and equipment should be reported to the Head of the Information and Technology (IT) Department.

The Institute's Operations Department has overall responsibility for the effective operation of this policy, and for ensuring compliance with the relevant regulatory framework. Day-to-day responsibility for operating and implementing this policy and ensuring its maintenance and review has been delegated to the Head of Information and Technology.

The IT department is responsible for:

a) The technical issues related to the access to, and use of Da Vinci's communication systems and equipment
b) Assisting management in intercepting communications and investigating matters of concern
c) Breach of the provisions of this policy; all outgoing email messages to contain The Institute's email legal notice

d) Scanning, filtering and blocking all electronic communications for damaging code such as viruses
e) The overall maintenance and management of this policy.

The Institute's Operations Department is responsible for the implementation, communication, maintenance and management of this policy, and disciplinary actions taken in terms of breach of this policy.

9. ACCEPTABLE USE OF SYSTEMS AND EQUIPMENT

Users are required to use The Institute's communication systems primarily for The Institute's business purposes. The Institute holds the right to block, intercept or monitor certain electronic communications including email and internet access for private and personal use. Common sense and judgement should guide personal and private usage. Permissible use should not impair the user's workflow or allow the communication system to become dysfunctional.

The Institute has the right to limit the size of incoming and outgoing email messages and attachments, downloads and other files, and may block and delete email messages, downloads, attachments or other files that are larger than the set maximum size.

It is the responsibility of users to limit the size of attachments and other files to prevent overloading of equipment.

The following should be considered with regards to email messages:

a) Email messages should be kept brief and formulated appropriately and directed only to the relevant individuals
b) Users must check email recipients prior to sending, forwarding or replying to messages. The sender should consider contacts who really need, or really should receive the email, or whether all recipients should be aware of each other
c) Users must decide before sending an email whether to copy a recipient 'cc' (carbon copy), or to blind copy 'bcc' (blind carbon copy) a recipient to the email when distribution lists are used, or if several contacts are copied in the same email
d) Users must always use the 'bcc' function when mailing to groups whenever the members of the group are unaware of the identity of all the other recipients (as in the case of marketing mailing lists), or where the user judges that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme). When the 'cc' box is used, each recipient is informed of the identity (and in the case of external recipients, the email address) of all the other recipients. Such a disclosure may breach any duty of confidentiality owed to each recipient, breach The Institute' obligations under the Protection of Personal Information Act, or may inadvertently

disclose confidential business information such as a marketing list. This applies to both external and internal email.

e) The subject field of an email message should relate directly to the contents or purpose of the message; users should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality, or breach of contract
f) Users should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Users should not:

g) Send or forward private work emails for a third party to read
h) Use their work email address for personal affairs/purposes
i) Use their own personal web based email account such as Gmail, Yahoo and Hotmail to send or receive email with business documents or content related to The Institute's business
j) Agree to terms, enter into contractual commitments, or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter
k) Send messages from another user's computer, or under an assumed name or conceal or misrepresents his/her name, unless specifically authorised
l) If users are out of the office for more than one day, they should activate the 'Out of Office' function to inform the sender of an email of the user's absence. The 'Out of Office' message should include both the period of absence and an alternative contact person's details
m) Users who receive a wrongly-delivered email should return it to the sender for acknowledgement
n) If a recipient asks the user to stop sending messages (whether of a personal nature or otherwise), the user should stop immediately
o) Access and use of third-party communication systems should be done in accordance with the third-party terms and conditions
p) Telephone conversations may be recorded by management of The Institute notifying parties in advance of the intention to do so.

10. UNACCEPTABLE USE OF SYSTEMS AND EQUIPMENT

Every user of The Institute's communication systems and equipment has a responsibility to maintain and enhance The Institute's public image and to use its systems in a productive manner. Any improper use of the communication system or equipment is not acceptable and will not be permitted. Access to The Institute's social network will only be granted for business purposes, and then subject to the conditions of the Social Media Policy. The following communication actions or forms of content are prohibited and subject to disciplinary action:

a) Modifying an e-mail message and forwarding or replying without noting the changes (i.e. deletions, removal of recipients, modification of content, etc.)
b) Fabricating a message to be forwarded
c) Intentionally bypassing the security mechanisms of the equipment or any third party security system or website
d) Modifying the internal mail transport mechanism to forge a routing path that a message takes through the Internet
e) Receiving and forwarding illegal content
f) Accessing, using, sending or sharing of confidential information about Da Vinci of any of Da Vinci's users or clients, unless expressly authorised
g) Participating in email 'chain letters', junk mail or similar activities
h) Agree to terms, enter into contractual commitments, or make representations by any communication facility unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter
i) Downloading, receiving and/or installing or utilise software applications not approved by the IT department
j) Knowingly burden Da Vinci's equipment or communication system with data unrelated to Da Vinci's official business (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server)
k) Contribute to communication facility congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them
l) Using automatic forwarding of emails (Auto Rules) to any person without such person's consent
m) The creation, sending or forwarding of unsolicited mail (spam)
n) The creation, sending or forwarding of marketing information or advertising material unrelated to Da Vinci's official business
o) Sending or forwarding messages and attachments that are infected with malicious codes such as viruses
p) Send messages from another person's e-mail address (unless authorised) or under an assumed name
q) Using removable media that may be infected with malicious code
r) Using any encryption, authentication and/or digital signatures not authorised by the IT department in writing
s) Downloading, reproducing, sharing, retaining and/or creating records that contain music, images, sound or video, if such record is not reasonably required for the user's official Da Vinci services
t) Copyrighted materials belonging to entities other than Da Vinci must be respected and managed in accordance with whatever license terms applicable
u) Accessing and using internet relay chat if such actions burden Da Vinci's equipment or communication system

v) Any actions that knowingly prevent other users from using and accessing equipment or communication systems
w) Access or participate in any Internet social network, unless specifically authorised by Da Vinci IT
x) Gambling using the Da Vinci communication facility
y) Taking any of the steps or actions criminalised and detailed in the Electronic Communications and Transactions Act including but not limited to hacking or developing, downloading and using any technology that may circumvent IT security measures
z) Any destructive and disruptive practices on, through, or with equipment or communication systems
aa) Indiscriminate storage and/or forwarding of e-mail, files, websites and attachments for which permission has not been obtained from the originator or copyright holder
bb) Any purposes that could reasonably be expected to cause directly or indirectly excessive strain on any computing facilities, or unwarranted or unsolicited interference with others
cc) Any activities utilising the equipment or communication systems which could damage Da Vinci's image, reputation and/or financial position
dd) Sending, replying to, or forwarding e-mail messages or other electronic communications which hide the identity of the sender, or represents the sender as someone else
ee) Reading, recording, copying or listening to messages and information delivered to another user's communication system without prior permission is prohibited
ff) Using or accessing Da Vinci's equipment or communication system to commit fraud or any other criminal offence(s)
gg) Sending or disclosing third party personal information without the authorisation of Da Vinci
hh) Sell or advertise using the communication facility, or broadcast messages about lost property, sponsorship or charitable appeals (unless authorised).

11. EQUIPMENT AND DATA SECURITY

a) Users are responsible for the security of the equipment allocated to, or used by them, and must not allow it to be used by anyone other than in accordance with this policy
b) Users are responsible for the security of their equipment and communication system. If leaving equipment unattended, or on leaving the office, they should ensure that they lock the equipment or log off or use screen savers with passwords to prevent unauthorised users accessing the system in their absence
c) Users without authorisation should only be allowed to use terminals under supervision
d) Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT Department

e) Passwords are unique to each user and must be changed regularly to ensure confidentiality
f) Passwords must be kept confidential and must not be made available, including, but not limited to sharing with anyone else
g) The user will be responsible for any action of a third party where the user has shared his/her password with the third party without proper authorisation
h) On termination of employment for any reason, staff must provide details of their passwords to the IT Department and return any equipment or access cards
i) A user must not try to circumvent login procedures on any equipment
j) Users should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the business or exposing it to risk
k) Users should not download or install software from external sources without authorisation from the Head of Information and Technology. This includes software programmes, instant messaging programmes, screensavers, photos, video clips and music files
l) Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff should seek advice from the IT department
m) No device or equipment should be attached to The Institute's systems without the prior approval of IT. This includes any USB flash drive, MP3 or similar device, Personal Digital Assistants (PDAs) or cellular telephones. It also includes use of the USB port, infra-red connection port or any other port
n) All emails passing through the system are monitored for viruses. Users should exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious (for example, if its name ends in .exe). The IT department should be informed immediately if a suspected virus is received. The Institute reserves the right to request a block on access to attachments to emails for the purpose of effective use of the system and for compliance with this policy
o) The Institute also reserves the right to request IT not to transmit any email messages. To avoid the accidental activation of any viruses in incoming email, emails should be viewed unopened with the default email inbox setting on 'preview' pane
p) Users should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised
q) Access to certain Internet sites may be blocked by IT. If the user has a legitimate business requirement to be able to access such Internet sites, this may be taken up with IT Management for authorisation.

12. WORKING REMOTELY (OFF-SITE)

Working remotely refers to the procedures when the user accesses The Institute's communication facilities or equipment off-site, working on Da Vinci business away from The Institute's premises.

No equipment may be removed from the premises without express written permission from the Head of Information and Technology.

When working remotely the user must:

Password-protect any work which relates to The Institute's business so that no other person can access it

a) Position him/her is such a way that the work cannot be overlooked by any other person
b) Take reasonable precautions to safeguard the security of The Institute's equipment, and keep their password secret
c) Inform the police and the IT department as soon as possible if either The Institute's equipment in the user's possession or any computer equipment on which Da Vinci work was done, has been stolen; ensure that any work which is done remotely is saved on the network or is transferred to the network system as soon as reasonably practicable
d) Mobile devices are easily stolen and not very secure so the user must password protect access to any such devices used, and on which is stored any personal data of which The Institute is responsible for, or any information relating to The Institute's business, clients or their business.

13. RIGHT TO MONITOR, INTERCEPT AND EXAMINE COMMUNICATION

a) The Institute's communication systems and equipment are made available for business purposes
b) The Institute respects the privacy of its employees, but holds the right to intercept, monitor and/or examine any communications and or records
c) The user's privacy will be limited during utilisation of the communication system and equipment
d) All communications executed on the communication system are seen as communications taking place in the course of carrying out The Institute's business, and are records of The Institute. The users should not assume that communications over the communication system are confidential
e) The Institute reserves the right to access and disclose as necessary all communications sent over its communication system, without regard to content. Since personal communications can be accessed by The Institute management without prior notice, users should not use communication systems to transmit any messages they would not want read by a third party
f) Back-up copies of communications may be maintained and referenced for business and legal reasons
g) Communications created, sent or received during a user's utilisation of The Institute's communication equipment may be made available to another user that has been appointed in the previous user's position

h) The Institute reserves the right to intercept or examine any communication and/or record if such interception or examination is reasonably required and justified for one or more of the following purposes:

I. Compliance with Da Vinci's obligations as detailed in this policy
II. Investigating, preventing or detecting unauthorised access or use
III. Investigating, preventing or detecting breach of the provisions of this policy
IV. Maintenance of the security of any equipment or communication system
V. Business continuity, disaster recovery or similar emergency measures
VI. Prevention of loss or destruction of The Institute's assets or data
VII. Investigating or detecting illegal activities
VIII. Legal/Court orders or warrants.

i) The Institute's right to intercept any communication for disciplinary or legal action shall:
   I. Only commence with the prior authority of the system controller, whose roles has been assigned by the Head of Information and Technology
   II. Be implemented with due regard to the privacy and constitutional freedom of users.

j) Any person who intercepts communications or has access to intercepted communications shall sign a non-disclosure agreement or clause prior to such interception, and undertake not to disclose the interception process, the identity of subject and/or any related information, unless authorised to do so by due legal process, or for the purposes of disciplinary or legal action

k) The Institute shall not share or disclose the following information to third parties:

   I. Private, personal and confidential information collected through the interception of communications
   II. The identity of users whose communications are, or were the subject of interception, unless such disclosure is authorised by due legal process or for the purposes of disciplinary or legal action
   III. Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software

14. RIGHT TO SEARCH

The Institute has the right to search a user and his/her equipment where any requirement of this policy has been breached. For this purpose, The Institute may utilise the services of a security company.

15. EMAIL SIGNATURES

Email messages are activated by the IT and Marketing department once a new signature has been approved for use and are required to have the following standard signature attached to all outgoing messages:

a) Name of Sender
b) Designation of Sender
c) Telephone Number
d) Mobile Number (where required for business purposes)
e) Email address
f) Da Vinci's Website address
g) Da Vinci's physical address
h) Email Disclaimer

16. EMAIL LEGAL NOTICE

a) All outgoing emails must have The Institute's standard email legal notice at the bottom of the message for all reasonable recipients to see and take note of the reference via the hyperlink. This email legal notice may not be removed or tampered with by users
b) The Institute's disclosure requirements are detailed as per the Companies Act of 2008 and other relevant regulations and rules
c) The Institute's legal disclaimer notice addresses the following detail:

    I. Confidentiality aspect
    II. Copyright matters
    III. Data and Privacy Protection
    IV. Agreements with The Institute
    V. Legally binding aspect
    VI. Opinions of the author of the email
    VII. Views and opinions of The Institute

d) The official Da Vinci disclaimer is to appear on emails sent:

    Disclaimer: The DaVinci Institute for Technology Management (Pty) Ltd is a registered private higher education institution under the Higher Education Act, 1997.

The information contained in this email is confidential and may be legally privileged. It is intended solely for the recipient to whom DaVinci has addressed this email. If you are not the intended recipient, you are hereby advised that any disclosure, distribution, or reliance on the contents of this email is strictly prohibited. DaVinci does not accept legal responsibility for the contents of this email, nor does any email or data message, sent or received, create a binding legal transaction. DaVinci shall not be liable for any harm or loss resulting from viruses in this email or its attachments, including data corruption. Additionally, DaVinci shall not be held liable for any offensive or defamatory statements or materials contained in this email. Any views or opinions expressed are solely those of the sender and do not represent DaVinci. All contents of this email, whether sent or received by DaVinci, shall be protected in accordance with the provisions of the Protection of Personal Information Act (4 of 2013) (POPIA). These terms apply to all emails sent and received by DaVinci, and this email disclaimer shall be governed by the laws of South Africa.

17. EMAIL FOR ADVERTISING/NEWSLETTER PURPOSES

a) The communication system shall only be used for advertising and/or newsletters by an authorised department, or alternatively, the authorised person to distribute it
b) All advertising and/or newsletters (in electronic format) shall contain the necessary 'unsubscribe' function at the bottom of the communication.

18. DUTY TO DISCLOSE AND REPORT BREACH OF PROVISIONS

a) Users have the duty to disclose all true or suspected attempts that may reasonably breach any provision of this policy to the Head of Information and Technology
b) Where certain events have to be reported to outside authorities, such reporting shall be done by authorised persons at The Institute
c) All incidents must be properly investigated by suitably trained and qualified personnel
d) Evidence relating to a breach of this policy must be properly collected and forwarded to the Head of Information and Technology.
e) A database of policy breaches should be created and maintained. The database should be studied regularly with the circumstantial evidence used to help reduce the risk and frequency of incidents at The Institute.
f) Any Data breach incidents should be emailed to databreach@davinci.ac.za which is captured and logged and escalated to the responsible department for action and review.

19. CONSEQUENCES OF MISCONDUCT

Failure and/or refusal to abide by the rules detailed in this policy shall be deemed as misconduct. The Institute may initiate the appropriate investigation and disciplinary action against users. Such steps may include dismissal and may further lead to criminal and/or civil prosecution.

20. POLICY CHANGES

The Institute reserves the right to amend this policy and shall ensure that all amendments are communicated to the users accordingly.

21. 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 head of Information and Technology.