POLICY ON
ELECTRONIC COMMUNICATIONS

Policy Owner	Chief Information Officer
Division/Unit/Department	Information Communications and Systems
Date of Initial Approval	25 April 2017
Approved by	MEC
Approval Dates of Revisions/Amendments [1]	17 October 2023
Next Review Date	17 October 2028
Platform to be published on	UJ Intranet

[1] Approval must be by the same structure that approved the initial Policy.

TABLE OF CONTENTS

1. PREAMBLE

In pursuit of its vision of being an international University of choice, anchored in Africa, dynamically shaping the future, stakeholders of the University of Johannesburg ("the University"/ "UJ") use the Information and Communication Technology ("ICT") systems owned or leased by the University extensively for purposes of communication. The laws on the employment relationship and on electronic communication, and the doctrine of vicarious liability entail risks for the University in that the University makes its ICTS available to its stakeholders for purpose of communication. Without effective control of the access to and use of its ICT systems, the University is exposed to risks of deliberate or accidental misuse of its facilities and disclosure of sensitive information to unauthorised parties. The UJ Electronic Communications Policy ("the Policy") provides a uniform framework to manage the risks associated with electronic communication using UJ ICT systems. Furthermore, to guide stakeholders of the University, on what constitutes fair use of the ICT Systems for communication as well as the responsibilities and accountabilities of the stakeholders.

2. PURPOSE

The purposes of this Policy are to:

2.1 make users aware of certain risks relating to communication using ICT systems.
2.2 raise the awareness of important security issues, to assist in respect of UJ's ICTS and assist all users in performing their duties in a secure way.
2.3 Inform and educate users on the regulatory limitations and create rules for the use of UJ's ICT systems.
2.4 provide for the interception of communications in line with legal requirements.
2.5 deal with matters incidental to the devices which are used or can be used to access UJ's ICTS for purposes of communication.
2.6 allocate roles and responsibilities to stakeholders in respect of UJ's ICT Systems for purposes of communication.
2.7 ensure and maintain the values and integrity of UJ's ICT Systems.
2.8 inform users of the potential consequences of not complying with the requirements of the Policy.

3. POLICY OBJECTIVES

The Policy creates:

3.1 uniform rules for the responsible and appropriate use of UJ's ICTS used for purposes of communication with the aim:
  3.1.1 to ensure UJ ICTS users recognise that UJ's ICTS provides an important medium of expression, the freedom of which is guaranteed by the Constitution, as is academic freedom, which freedom is not absolute, but restrained, amongst others, by the rights and freedom of others.
  3.1.2 to prevent or reduce the risk of the University suffering damage (including reputational damage) or incur liabilities from third parties.
  3.1.3 to manage the interactions, functionality, and responsibilities of stakeholders in respect of the UJ's ICTS used for purposes of

communication.

4. SCOPE

This Policy applies to all users who are provided with access to UJ's ICT systems.

5. ABBREVIATIONS AND DEFINITIONS

For this Policy, unless it is stated otherwise or the context indicates otherwise, the following abbreviations and terms will bear the following meanings, and other grammatical forms of the terms have corresponding meanings:

No.	Abbreviation	Definition
5.1	Data	The electronic representation of information in any form.
5.2	Communication	Includes both direct communication and an indirect communication.
5.3	Direct communication	Oral communication, other than an *indirect communication*, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication.
5.4	ICS Division	Information and Communication Systems Division.
5.5	ICT	Information and Communication Technology.
5.6	ICTS	ICT Systems comprised of a wide range of ever evolving and converging technologies that store, retrieve, manipulate, transmit and receive information electronically in a digital format, including the software associated therewith. The components of the ICTS are located on UJ's premises and elsewhere, may be owned or leased by the University, may behosted by third-parties, and include devices such as servers, data lines, voice lines, and devices which can be stand-alone or connected to a voice or data line, like desktop computers, laptops, notebooks, tablets, telephones, smart phones and facsimile machines, and some of the devices which are the property of third parties (including users) can also be connected to the ICTS.
5.7	Indirect communication	The transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds, data, text, visual images, whether animated or not, signals, or radio frequency spectrum or in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system
5.8	Intercept	The acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the monitoring of any

		such communication by means of a monitoring device, viewing, examination or inspection of the contents of any indirect communication and diversion of any indirect communication from its intended destination to any other destination, and “interception” has a corresponding meaning.
5.9	IT Service Desk	Information Technology Service Desk
5.10	Management requirements	A set of techniques organizations employ to ensure they achieve important business goals and meet customer requirements throughout the product life cycle.
5.11	MEC	Management Executive Committee of the University
5.12	NDA	Non-Discloser Agreement
5.13	NPI	National Provider Identifier
5.14	PIN	Personal Identifiable Number
5.15	Policy	The Electronic Communications Policy
5.16	PRCC	Project and Resourcing Committee of Council
5.17	Records	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 any User of the ICTS, regardless of the format thereof.
5.18	Security mechanism	Technical tools and techniques that are used to implement security services.
5.19	Service level	Is the metrics by which a particular service is measured.
5.20	SMP	Social Media Platform
5.21	SMS	Short Message Services is a technology for sending text messages between mobile phones.
5.22	Stakeholders	All University employees, persons who hold special UJ appointments, students (including students in residences or belonging to societies), alumni, visitors, contractors, service providers, consultants, associates, and others who are granted access to use UJ’s ICTS.
5.23	University/ UJ	University of Johannesburg.
5.24	User	A stakeholder to whom access is granted to use UJ’s ICTS.
5.25	VC	Vice-chancellor and Principal of the University.
5.26	VPN	Virtual Private Network is the opportunity to establish a protected network connection when using public networks. VPNs encrypt the internet traffic and disguise online identity.

5.27	Wrongful	Without detracting from the meaning of the expression in common law and limiting its meaning, "[a]n enquiry into wrongfulness is determined by weighing competing norms and interests. The criterion of wrongfulness ultimately depends on a judicial determination of whether it would be reasonable to impose liability *on a defendant* flowing from specific conduct. Whether conduct is wrongful is tested against the legal convictions of the community which are 'by necessity underpinned and informed by the norms and values of our society, embodied in the Constitution'" *Oppelt v* Department ofHealth*, Western Cape* 2016 1 SA 325 (CC) 349 (words not relevant for present purposes, omitted)

6. PRINCIPLES

The Policy is underpinned by the following principles:

6.1 the University recognizes, respects and protects all constitutional rights and freedoms of the Stakeholders, including their rights to privacy and freedom to receive and impart with information (including academic freedom).

6.2 UJ's ICT systems are provided for, and in connection with, the business of the University and must be used for that purpose. UJ's ICTS remain the University's property or possession (if always leased by the University), including components of the ICTS acquired by the University from research funding and research contract funding. The University has a legal right and duty to:

6.2.1 secure and maintain its ICTS and all components forming part thereof.

6.2.2 ensure the confidentiality of its trade secrets, students, employees and confidential information generally.

6.2.3 protect the privacy of its stakeholders.

6.2.4 identify and address the potential risks associated with the use of ICT and ICTS in the workplace.

6.2.5 comply with the provisions of laws and regulations that govern the access, use and interception of communications.

6.2.6 investigate and take steps (including legal and disciplinary steps) in respect of unlawful or unauthorised use of its ICT and Systems.

6.2.7 to access, review and monitor all components of its ICT and ICTS subject to the law and the Policy.

7. POLICY STATEMENTS

7.1 The use of UJ ICTS for communication

7.1.1 When acting in the course and scope of their employment, all employees of the University may and should use UJ's ICTS for communication and they must do so whenthey use e-mail facilities in the course and scope of their employment. E-mail messages and attachments form part of the business records of the University and must be retainedby the University, whilst the University has no access to, or control over the security of, third-party e-mail systems and storage servers provided, for e.g., by Yahoo, Gmail, Hotcom, etc and messages sent from such systems do not contain the UJ's e-mail legal notice.

7.1.2 All members of staff, in particular academic and research staff, may, and should, use their UJ address (including UJ e-mail address) and UJ designation when publishing the results of their research and scholarly work and in popular media, and when doing so they neither need, nor are they presumed to have, institutional endorsement for their views, arguments and results.

7.1.3 The University permits limited use of its ICTS for non-business purposes by Users. This permission is granted as a privilege, and not as a right. This being the case, the University may at any time withdraw such permission at its sole discretion, either generally or in respect of a specific User or component of its ICTS.

7.1.4 When using UJ's ICTS for purposes of communication other than for the business of the University, members of staff must be alert to the fact that members of the public may nevertheless associate the contents of such communication with the University, which may give the University an interest in such communication. The more likely it is for members of the public to associate an employee of the University with the University, the more such employee must be alert to this issue. Members of the Executive Leadership Group should particularly have regard to the extent which, and if, their communications could/can be divorced from their offices, i.e., the extent to which they can enter the public domain in their personal, as opposed to office-related, capacities.

7.1.5 Nobody may use a UJ letterhead, or any UJ designation (including a UJ designation in an electronic signature) for private communications or for private work (even if approved private work).

7.1.6 Users who are not UJ employees must read and agree to abide by the Policy and related policies before access to UJ's ICTS is authorised. They must also sign a non-disclosure agreement (NDA).

7.1.7 To ensure that users are accountable and to prevent abuse of UJ's ICTS, e.g., by persons representing themselves as UJ employees or a particular UJ employee and thereby claiming authority they do not have, the following conduct is forbidden:

7.1.7.1 using someone else's user id and password to access the ICTS.

7.1.7.2 pretending to be someone else on the telephone or by email.

7.1.7.3 using someone else's PIN.

7.2 User access authorisation

7.2.1 All stakeholders wishing to obtain access to UJ's ICTS must obtain prior written approval from their line manager before such access is granted.

7.2.2 Passwords must be used according to UJ's Access Management Policy and Standard.

7.3 Duties of employees in respect of all forms of communication, including electronic communication.

7.2.3 The contents of communication must always comply with the University's rules, regulations, policies and practices.

7.2.4 It is expected that those who communicate on behalf of the University do so in a professional way consistent with their assigned duties, comply with the UJ values and act within their scope of authority.

7.2.5 An expression of personal opinion must, where relevant, reflect that fact, mindful that such a disclaimer does not necessarily exempt a person from accountability of responsibility towards the University.

7.2.6 Provided that they are wrongful and there is no demonstrable need on the basis of academic freedom therefore, communication is prohibited which:

7.3.1.1 is or may be detrimental or injurious to the University's image, brand, reputation and relationships with others or groups.

7.3.1.2 is intended or may have the effect of inciting violence or advocate hatred.

7.3.1.3 is or may be threatening, obscene, oppressive, offensive, vulgar, profane, defamatory, discriminatory, racist, pornographic, harassing or otherwise wrongful.

7.3.1.4 is a violation of intellectual property rights or privacy laws.

7.3.1.5 bring or may bring the University or any person employed by or attending the University into disrepute.

7.3.1.6 indicates or gains support for any religious or political purpose.

7.4 Email communication

7.4.1 Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner.

7.4.2 UJ reserves the right to review, audit, access and disclose all messages created, received, or sent over the e-mail.

7.4.3 E-mail access will be terminated when the employee terminates his\her employment contract with UJ.

7.4.4 The e-mail legal notice, e-mail messages and attachments form part of the business records of the University and must be retained by the University.

7.4.5 The University has no access to, or control over the security of, third-party e-mail systems and storage servers provided, for *e.g.,* by yahoo, gmail, hotmail, etc. and messages sent from such systems do not contain or subject to the UJ's e-mail legal notice.

7.4.6 All members of academic and research staff, may, and should, use their UJ address (including UJ e-mail address) and UJ designation when publishing the results of their research and scholarly work and in popular media, and when doing so they neither need, nor are they presumed to have, institutional endorsement for their views, arguments and results.

7.4.7 All outgoing e-mail messages must display a hyperlink to UJ's e-mail legal notice at the bottom of the e-mail message and users may not remove or attempt to remove such hyperlink in any manner whatsoever.

7.5 Interception of communication

7.5.1 The University is entitled by law to intercept indirect business communications. Indirect business communications which are intercepted by the University having regard to past precedents, generally fall in the following categories:

7.5.1.1 communications related to criminal activities.

7.5.1.2 communications related to misconduct giving rise to disciplinary proceedings.

7.5.1.3 communications to establish facts related to the business of the University.

7.5.1.4 The University is entitled by law to intercept, in the course of carrying on of its business, any indirect communication:

7.5.1.4.1 by means of which a transaction is entered into in the course of its business.

7.5.1.4.2 which otherwise relates to its business.

7.5.1.4.3 which otherwise takes place in the course of the carrying on of its business, in the course of its transmission over a telecommunication system.

7.5.2 The University may only intercept an indirect communication:

7.5.2.1 if such interception is affected by, or with the express or implied consent of the VC, for purposes of:

7.5.2.1.1 monitoring or keeping a record of indirect communications.

7.5.2.1.2 in order to establish the existence of facts.

7.5.2.1.3 for purposes of investigating or detecting the unauthorised use of that telecommunication system.

7.5.2.1.4 where that is undertaken to secure, or as an inherent part of, the effective operation of the system.

7.5.2.1.5 monitoring indirect communications made to a confidential voice telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose.

7.5.3 The VC or any person authorised by him/ her, will make all reasonable efforts to inform users, who intend to use its ICT and ICTS, that indirect communications transmitted by means thereof may be intercepted, provided that indirect communication may also be intercepted with the express or implied consent of the person who uses that telecommunication system.

7.5.4 The University's right to intercept communication as aforesaid, is continuous.

7.5.5 The interception of direct communication is regulated by law. Any person (other than a law enforcement officer in respect of whom special provisions apply), may intercept any communication if he or she is part of the communication, unless such communication is intercepted by such person for purposes of committing an offence.

7.5.6 Nothing in this Policy derogates from any other rights of interception of communication which the University has in law.

7.5.7 The VC will as far as possible, seek a resolution from the MEC to intercept any indirect communication. The MEC must consider whether there are reasons to intercept the communication without the consent of the user.

7.5.8 The MEC will submit at least once a year reports in respect of indirect communications that were intercepted of academic members of staff and other members of staff respectively to the Projects and Risk Committee of Council (PRCC), which committee exercises governance functions in respect of the ICTS and services. The Representatives of Senate serving on Council are invited to attend the relevant meeting of the PRCC in respect of the agenda item pertaining to the interception of communication of academic members of staff. The reports must provide details of the number of users in respect of whom communication was intercepted, the grounds on which the interception was undertaken, the purposes of the interception, whether it was considered to obtain the prior consent of the user for the interception, what the reason for an interception without consent was and any other information that may be relevant.The names of the users do not need to be supplied.

7.5.9 Compliance with the oversight mechanisms has no effect on the lawfulness of any interception that otherwise complied with the legal requirements for interception.

7.5.10 Any person who actually intercepts indirect communication and has access to intercepted communication must treat such information as strictly confidential.

7.5.11 The University will not share with or disclose to third parties private and personal information obtained by intercepting indirect communication which are not the business of the University unless it is permitted by, or required by law, for example, for purposes of legal or disciplinary proceedings.

7.5.12 Compliance with the additional measures to minimize the impact of interception has no effect on the lawfulness of any interception that otherwise complied with the legal requirements for interception.

7.6 Use of UJ's ICTS for purposes of communication other than the business of the University

7.6.1 Users must use UJ's ICTS primarily for UJ's business purposes and to perform the duties assigned to them. Incidental and occasional private and personal use, in moderation, will be tolerated, subject to the rules detailed in this Policy. Common sense and good judgment should guide personal and private usage, without limiting the generality of the aforesaid, personal and

private usage will be tolerated if:

7.6.1.1 it is reasonable and not excessive.

7.6.1.2 it does not consume a lot of system resources (e.g., by sending large files, or many messages via e-mail, or consuming large quantities of internet bandwidth).

7.6.1.3 it does not interfere with the performance of the duties as a staff member.

7.6.1.4 it does not interfere with the productivity or performance of other stakeholders or infringe upon their rights.

7.6.1.5 it does not expose the University to any legal liability or cause it any damage (including reputational damage).

7.6.1.6 it does not cause disruptions to the operations or resources of UJ's ICS Division.

7.6.1.7 it does not violate any other provision of this Policy or any other applicable policy, guideline or rule of UJ.

7.6.1.8 it does not prejudice any UJ business activity, whether deliberate or accidental.

7.6.1.9 UJ's ICTS is used to create, send, receive or store private or personal communicationor records, in order to protect the privacy of any such communications or records, the user should clearly mark such communication and records as "Private", however, users must understand that their right to privacy in their personal records under these circumstances is subject to UJ's right to protect its business interests as provided in law and Policy.

7.7 Use of personal mobile devices

7.7.1 The University allows users to access UJ ICTS from their personal devices to improve productivity and flexibility, however, users must be cautious of the following:

7.7.1.1 must always ensure that the devices used to access ICTS is always password protected.

7.7.1.2 use an encryption feature to encrypt the data on mobile devices.

7.7.1.3 keep applications and systems up to date with the latest security patches.

7.7.1.4 must separate applications for personal and work when accessing ICTS, to allow the application to be removed when no longer employed by UJ.

7.7.1.5 UJ employees must use UJ-approved cloud storage services to store UJ data.

7.7.1.6 The university must utilize the Short Message Services (SMS) system, managed by the ICS Division, to provide communication with registered students. The system allows only authorised users to compile and send messages to students and is only used for official communication.

7.8 Telephone communication

7.8.1 The ICS Division is responsible for issuing telephone devices to UJ employees to ensure efficient and effective communication amongst employees and UJ stakeholders.
7.8.2 The line manager must determine which employees must have telephone devices.
7.8.3 UJ employees must be given a unique PIN code to make official calls and if an employee feels that the PIN code has been compromised, they must contact the ICS Division for assistance.
7.8.4 The ICS Division must issue an electronic record of all the calls made and billing for the month to all employees with telephone devices.
7.8.5 The University allows private use of the telephone but should be limited.
7.8.6 The University telephone may not be used to conduct illegal activities.

7.9 Social media communication

7.9.1 The University uses Social Media Platforms (SMP) to pursue its vision, mission and strategic objectives. The contents uploaded to the UJ SMPs must always be consistent with the University's values.
7.9.2 The University allows all users to participate in all SMPs, however, it is their responsibility to ensure that it does not interfere with their performance.
7.9.3 UJ users must not create Social Media accounts on behalf of the University, the University has a communications department that will communicate on behalf of the University.
7.9.4 UJ users must be aware that the content uploaded to social media platforms is public, can be accessed globally, downloaded and further distributed, and is usually permanent, even if deleted. Therefore, users must always comply and adhere to all UJ policies, regulations, acts and laws when taking part in social media.
7.9.5 To protect the brand, UJ has the right to monitor all social media posts and take appropriate action where possible by following the internal disciplinary procedures.
7.9.6 In compliance with UJ's record retention policies, social media content may be retained in UJ's archives, or as backup copies, even after they are deleted from an employee's SMP. The goals of the backup and archiving procedures are to ensure system reliability, prevent document and data loss, comply with regulatory and legal requirements, and supply evidence in the event of litigation.

7.10 Internet and intranet usage

7.10.1 UJ's internet access is controlled through individual accounts and passwords. ICS Division is responsible for defining appropriate internet access levels for UJ users.
7.10.2 UJ users are encouraged to use the internet to further the goals and objectives of UJ. The types of activities include:
7.10.2.1 communicating with users within the context of an individual's assigned responsibilities.

7.10.2.2 acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.

7.10.2.3 Participating in educational or professional development activities.

7.10.3 UJ users must treat all other individuals, clients, employees, etc. that they interact with in any virtual, online forum, or network capacity in accordance with human rights codes, UJ values, policies, and basic corporate social decorum.

7.10.4 UJ Head of Department is responsible for defining appropriate internet access levels for employees in their department and conveying that information to the ICS Department.

7.11 Collaboration facilities

7.11.1 UJ users are encouraged to use collaboration facilities approved by the University to enhance collaboration and productivity. File-sharing activities may include organising and storing information related to permanent roles/projects.

7.11.2 Electronic records that contain evidence of official transactions (i.e., records) must be backed up and migrated for longer-term retention.

7.11.3 Data used must be kept confidential and secure by the user and not shared unless there is a business need to do so.

7.11.4 UJ must archive and dispose of records in accordance with its retention schedule.

7.11.5 To maximize flexibility for users, sites should be created by team leaders and appoint administrators to manage the site on a contingency basis.

7.11.6 All files must be retained after user accounts are deleted. The departing employee's manager must have access to the files.

8 PROTECTION OF DEVICES CONTAINING RECORDS OF COMMUNICATION

8.1 Users must take reasonable and appropriate measures to protect the components of UJ's ICTS (including devices providing access to the ICTS, like computers) against accidental or malicious destruction, damage, or unlawful modification. Where possible, all devices must be physically secured to a desk or similar object with a security cable. In the case of desktops and devices, users must ensure as far as possible that the office in which the desktop computer resides is adequately secured at the close of business or while left unattended. UJ is not liable for the loss or theft of personal devices, which is a further reason why individuals must take care of their property. Where any UJ devices are lost or stolen, it must be reported immediately to the line manager and the UJ IT Service Desk so that appropriate steps can be taken, for example, insurance claims and removal of logical access.

8.2 Users must take reasonable and appropriate measures to protect the disclosure of records stored on UJ's ICTS or on devices not owned or leased by UJ on which UJ records are stored (e.g., personal cell phones or tablets linked to UJ's e-mail system, or USB memory sticks and other devices on which UJ records are stored), and to maintain appropriate levels of confidentiality, integrity and availability of record stored on them. For this purpose, personal passwords must be kept safe, open sessions terminated,

password-protected screensavers used which activate automatically after a period of inactivity, electronic communications facilities must be logged out from when such systems are left unattended, and encryption tools or techniques used and authorised by UJ's ICS Division. Where personal property is lost or stolen on which UJ records are stored, it must be reported immediately to the IT Service Desk so that appropriate steps can be taken, for example, removal of logical access.

8.3 Mobile devices (e.g., laptops, tablets and cellphones) and other devices used to work remotely, whether or not the property of UJ, which can be used to link to UJ's ICTS or contain UJ records, pose considerable risks for the University, which requires users to take reasonable and appropriate steps to guard against the loss or theft of the devices and the disclosure of UJ records stored on them. Without limiting the reasonable and appropriate steps that may be required, the following examples are provided:

8.1.1 ensuring that devices used for remote work are adequately secured and remain out of sight, both when travelling and when working at, or storing the devices at a location other than UJ premises.

8.1.2 ensuring that UJ devices are not used by non-UJ personnel.

8.1.3 being careful when devices that are personal property linked to UJ's ICTS or containing UJ records are used by others, e.g., do not allow strangers to use them or supervise the use.

8.1.4 ensuring that confidential information is not inadvertently viewed by third parties (e.g., when using laptops on public transport or in airport lounges).

8.1.5 ensuring that confidential information stored on mobile devices is password protected or encrypted.

8.1.6 taking steps to ensure that any UJ information stored on computers or mobile devices used to work remotely (such as laptops, personal organisers, USB memory sticks or mobile phones) is regularly backed up.

8.1.7 guarding against unintentional disclosure of the University information while working in public places, e.g., on aeroplanes, airport lounges, restaurants or other public areas. Users must take all reasonable steps to preclude onlookers from viewing any sensitive or important University information. Similarly, users should take care when communicating via mobile phones and telephones.

8.1.8 using suitable techniques (*e.g.,* through encryption mechanisms approved by the ICS Division) to protect the University's information stored on mobile devices (such as laptops, USB memory sticks and mobile phones) and home computers from disclosure.

8.1.9 minimising (including when travelling), the risk of mobile equipment theft, by not leaving them in unattended motor vehicles and other forms of transport, hotel rooms, conference centres, meeting places or public places.

8.1.10 physically securing laptops to a desk or similar object with a suitable security cable or storing it in a locked cabinet outside of normal working hours or when left unattended.

8.1.11 the University has the right to recover from users' losses suffered to any components of its ICTS (including computers and laptops) as a result of a user's negligence.

8.1.12 whenever a user wishes to temporarily remove computer equipment which can be connected or is connected to UJ's ICTS from UJ premises (not a user who has been allocated laptop computers and mobile devices), a written authorisation is required from the Business Manager or Executive Director. In the event that authorisation is obtained,such equipment must be returned in the same physical condition and within an agreed period.

8.1.13 all components of UJ's ICTS allocated to a user, including computing equipment which is or can be connected to UJ's ICTS, must be returned to UJ upon the termination of the legal relationship between UJ and a user for any cause whatsoever. It is the duty and responsibility of a user whose employment with UJ is terminated to return such components and to remove all information that is not related to the business of the University from them since it is not the intention of the University to retain such information, particularly private and personal information of a user. UJ accepts no responsibility with regards to a user's private and personal information stored on its devices; it is therefore the responsibility of the user to ensure that such information is at all times backed up to a personal storage device. Users are encouraged to ensure that persons who may need to access such private and personal information, including their next-of-kin and the executors of their estates, have access to such personal storage devices and are provided with the passwords to access those personal devices. All UJ devices shall, upon return, be wipedclean of any stored information and re-allocated. Before wiping such devices clean, UJ may at its discretion back up any information stored on them to other devices for purposes of business continuity. In the event of the death of an employee and in order to respect the confidentiality of the personal information of a deceased member of staff, the Executive Director responsible for human relations in consultation with the deceased's line manager has the power to determine which information does not relate to the business of the University and will be discarded, and which information relates to the business of the University and will be downloaded to other devices.

8.1.14 users must comply with the terms and conditions of the licenses in respect of the software provided by the University and respect the copyright that applies to such software and software developed by the University in which copyright vests in the University. UJ-licensed and UJ-owned software may not be copied to other devices without the authority of the CIO. Modifying, revising, adapting, translating, reverse-engineering or disassembling software is prohibited.

9 ELECTRONIC EVIDENCE

UJ has the legal right and duty to retain, collect, preserve and present electronic evidence to assist law enforcement agencies with internal investigations of data theft and policy violations.

UJ must maintain electronic evidence to assist in any investigations but not limited to:

- assist with the disciplinary proceeding to prove any wrongdoing or violation of policy.

- use as evidence in civil and criminal litigation.
- investigations of unauthorised system access.
- Demanded by civil discovery procedures, third party subpoena and/or court order.

9.1 Retention Of Potential Electronic Evidence

9.1.1 In order to ensure that UJ retains all potential electronic evidence, it shall retain and archivethe following Data Messages for the following periods:

9.1.1.1 Sent email messages for a minimum period of 3 years from the date the emailmessage was sent.

9.1.1.2 Received email messages for a minimum period of 3 years from the date the email message was received.

9.1.1.3 System Activity Logs files shall be retained for a period of 3 years from the date of the activity log.

9.1.2 The abovementioned Data Messages shall be retained and archived according to the following standards and guidelines, provided for in sections 15, 16 and 17 of the Electronic Communications and Transactions Act 25 of 2002:

9.1.1.4 Data Messages shall be retained and archived in their original format.

9.1.1.5 Email messages shall be retained and archives with Message Headers intact and unchanged.

9.1.1.6 Meta data inherent in the Data Message such as the identity of the creator, sender or recipient of the Data Message and the date of creation, sending or receipt shall be retained and archived with the Data Message unchanged.

9.1.1.7 The full integrity of the Data Message shall be retained.

9.1.1.8 Retained and archived Data Messages shall be secured and protected from unauthorised access or tampering.

9.1.1.9 Any changes to or attempts to change or tamper with retained and archived Data Messages shall be logged and retained for the duration of retention of the Data Message in question.

9.2 Consent to interception and monitoring

To comply with the requirements of section 5 of the Regulation of Interception of Communications Act 70 of 2002, all employees shall provide written consent to the interception and monitoring of all communications and system activities.

9.3 Identification, collection, preservation and presentation of Electronic Evidence

All requests for Electronic Evidence of whatsoever nature and for whatsoever purpose shall be directed to the Evidence Officer who shall identify, collect, preserve and present the required electronic evidence as provided for in this Policy.

9.4 Presentation of Electronic Evidence

9.4.1 For presentation purposes, electronic evidence is classified into two

categories, namely) business related evidence (such as business emails and electronic business records) and

9.4.2 Personal evidence (such as personal emails, website visits, personal instant messages and personal sms); and

9.4.3 In terms of the common law of evidence, all kinds of evidence may be classified into two further categories namely) evidence proving that data was sent, received, stored or tampered with (for example email message headers and audit logs), and ii) evidence proving the contents thereof (for example email and electronic records).

9.4.4 Presenting Evidence

9.4.1.1 Presenting business and/or personal evidence that Proves that information was sent, received or stored. Presentation of this kind of evidence is governed by section 15(4) of the Electronic Communications and Transactions Act 25 of 2002 and presented in the following manner:

- A printout of the evidence; and
- Certified as correct by the person who made the printout.

9.4.1.2 Presenting business evidence that proves the contents thereof. Presentation of this kind of evidence is governed by section 15(4) of the Electronic Communications and Transactions Act 25 of 2002 and presented in the following manner:

- A printout of the evidence; and
- Certified as correct by the person who made the printout.

9.4.1.3 Presenting personal evidence that proves the contents thereof. Presentation of this kind of evidence is governed generally by section 15 of the Electronic Communications and Transactions Act 25 of 2002 and the common law and presented in the following manner:

- A printout of the evidence;
- An affidavit by the person who created and received the evidence confirming that it was so created, sent or received; and
- Such person should also be available to give evidence and answer cross-examination in the proceedings the evidence is to be used in.

10 COMPLIANCE WITH ACTS AND REGULATIONS

10.1 The University must ensure that appropriate measures and controls are in place to ensure the confidentiality and integrity of personal information when being processed.

10.2 The University must provide law enforcement with the necessary technical assistance to search for, access or seize any ICT resources that may have been linked to cybercrime.

10.3 The University must report any offence to law enforcement and preserve any information that may assist with the investigation if it suspects that a crime may have been committed using its ICT resources.

10.4 The University has the right to capture and inspect any data stored or transmitted on its ICT facilities (regardless of data ownership) when:

10.4.1 investigating system problems or potential security violations.

10.4.2 maintaining system security and integrity.

10.4.3 detecting, preventing or minimizing unacceptable behaviour in its facilities.

10.4.4 such data will not be released to persons within or outside of the University, except in response to a lawful request.

11 ELECTRONIC COMMUNICATION SECURITY AND MONITORING

11.1 Any information that is deemed confidential and/or proprietary to UJ may only be transmitted via the UJ ICTS when suitable measures have been employed to ensure the confidentiality of such information. As a minimum sensitive information should be sent in a password-protected zip file, the password must be sent to the recipient by Short Message System (SMS) or telephonically. Encryption and the use of a Virtual Private Network (VPN) can also be considered.

11.2 When communicating via a voice network (e.g., telephone) and confidentiality is at stake, the user must verify the identity of the individual (by asking security questions) and ensure that the individual is authorised to receive any information deemed confidential and/or proprietary to UJ.

11.3 When remote access to sensitive and confidential information stored on UJ facilities is required, users may not e-mail that information to a system not controlled by UJ and are encouraged to apply to the ICS Division for VPN access rather than e-mailing it to their UJ e-mail account.

11.4 UJ has the right to limit the size of incoming and outgoing electronic messages and attachments, downloads and other files, and may block and delete e-mail messages, downloads, attachments or other files that are larger than the set maximum size. It is the responsibility of the user to limit the size of attachments and other files to prevent the overloading of UJ's ICTS.

11.5 UJ has the right to limit the nature and content of incoming and outgoing electronic messages.

11.6 UJ retains the right to monitor traffic on all data and other lines owned or leased by the University and prepare reports in that respect (for e.g., reports on the use of telephone lines detailing the date, time and duration of calls made from and to a specific telephone number, and the telephone numbers which were dialled or from which calls were received).

11.7 Anti-virus management software installed on UJ devices must be kept up to date by regularly connecting the devices to the ICTS.

11.8 Approved software installed on UJ devices must be updated on a regular basis. If a user believes that a particular software product, whether freeware, shareware or proprietary software, would assist in the furtherance of UJ's business, then motivation should be sent to the CIO.

11.9 Cryptographic mechanisms must be implemented to prevent unauthorized disclosure of NPI during transmission unless otherwise protected by alternative physical safeguards.

11.10 The University will establish and manage cryptographic keys for cryptography employed in the information system. Cryptographic keys should

be protected throughout their whole lifecycle.

11.11 The University must control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

11.12 All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure.

11.13 Equipment used to generate, store, and archive keys should be physically protected.

11.14 Network segregation must be implemented. Groups of information services, users, and information systems must be separated from one another.

11.15 The University must implement limitations and controls of network ports, protocols, and services.

11.16 Controls must be implemented to ensure information security in networks and protect connected services from unauthorized access. In particular, the following items should be considered:

- 11.16.1 responsibilities and procedures for the management of networking equipment must be established.
- 11.16.2 special controls must be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks.
- 11.16.3 appropriate logging and monitoring must be applied to enable the recording and detection of actions that may affect, or are relevant to, information security.
- 11.16.4 management activities should be closely coordinated both to optimize the service to the University and to ensure that controls are consistently applied across the information processing infrastructure.

11.17 Network connections associated with communications sessions must be terminated at the end of the sessions or after a defined period of inactivity.

11.18 The University must protect the authenticity of communications sessions.

11.19 The University must protect the confidentiality of NPI at rest.

11.20 Unauthorized and unintended information transfer via shared system resources must be prevented.

11.21 The University must prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.

11.22 The University must implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

11.23 Network communications traffic must be denied by default and network communications traffic must be allowed by exception (i.e., deny all, permit by exception).

11.24 External parties must agree to the secure transfer of business data with the University.

11.25 Appropriate policies, procedures, and controls must be established around the protection of information being transferred through various types of facilities.

11.26 All information transferred in electronic messaging must be properly protected.

11.27 Any confidentiality or non-disclosure agreements of the organization must be acknowledged, reviewed often, and documented.

11.28 The University has the right to monitor all calls to determine misuse or abuse of the telephone.

11.29 The University must use appropriate technical and organizational measures to safeguard personal information.

12 ROLES AND RESPONSIBILITIES

Role	Responsibilities
CIO	Is responsible and accountable for all UJ ICT policies.
ICS Division	Is responsible for: • implementing and maintaining the IT controls, systems and security standards. • assisting UJ's management in intercepting communications and investigating breaches of the provisions of this Policy. • ensuring all UJ's outgoing e-mail messages contain UJ's official e-mail legal notice available as a hyperlink from the bottom of such messages. • scanning and filtering all electronic communications for damaging code such as malware and blocking them if detected. • implementing a decision to intercept and monitor communication as provided for by law and in terms of the Policy.
ICT Strategy and Governance Unit	Is responsible for creating, reviewing, updating and maintaining this policy, including conducting Awareness and Training for UJ users.
MEC	Is responsible for providing support to the implementation of the policy.
Users	Are required to familiarise themselves with this Policy and adhere to and comply with its requirements. Users must report known or suspected violation of the provisions of this Policy to the UJICS Division or their line manager.
ICS Technicians	The technical employees appointed by UJ must maintain and support UJ's ICTS, its components and UJ devices which are or can be connected.

13 POLICY VIOLATION

Failure and /or refusal to comply with the provisions of this Policy may amount to misconduct and may result in disciplinary proceedings and /or dismissal in line with UJ's disciplinary code.

14 DEVIATION FROM THE POLICY

The CIO or the MEC must approve any deviation from the Policy, depending on the nature of the deviation sought.

15 POLICY REVIEW

The Policy review must be conducted every five (5) years in accordance with the approved University Policy on Policy Development and take place under the auspices of the official custodian of this policy, namely the Chief Information Officer.

16 RELATED DOCUMENTS

16.1 UJ Documents

16.1.1 Electronic Evidence Policy
16.1.2 IT User Access Management Standard
16.1.3 ICT Acceptable Use Policy
16.1.4 Information Security Policy
16.1.5 UJ Policy on Data Management and The Protection of Personal Information
16.1.6 UJ Protocol on the Protection of Personal Information
16.1.7 UJ Protocol for Data Management
16.1.8 UJ Statute
16.1.9 UJ Terms and Conditions of Employment
16.1.10 UJ Employee Code of Conduct
16.1.11 UJ Risk Management Policy
16.1.12 UJ Vision, Mission and Values

16.2 Other related documents

16.2.1 Cybercrimes Act 19 of 2020
16.2.2 Electronic Communications and Transaction Act 2 of 2003
16.2.3 Protection of Personal Information Act 4 of 2013
16.2.4 Electronic Communications Act 36 of 2005
16.2.5 Electronic Communications and Transactions Act 25 of 2002 (ECTA)
16.2.6 The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70of 2002
16.2.7 Protection of Personal Information Act 4 of 2013 (POPIA)
16.2.8 Constitution of the Republic of South Africa of 1996

Approval History Table	
Name of Approval Body (Committee)	**Date that the review was approved**
MEC	25 April 2017
MEC	17 October 2023