ELECTRONIC COMMUNICATIONS POLICY

Document number	
Custodian/Responsible Executive	**Executive Director: ICS**
Responsible Division	**ICS**
Status	Approval
Approved by	MEC
Date of Approval	25 April 2017
Amendments	31 October 2017
Date of Amendments	
Review date	**2020**

RELATED DOCUMENTS

UJ Documents (e.g. Policies, Regulations, Guidelines, Contracts)	**Other** (e.g. Legislation, DoE and HEQC directives and guidelines)
• **UJ Statute;** • **UJ Terms and Conditions of Employment;** • **UJ Employee Code of Conduct;** • **UJ Risk Management Model;** • **UJ Risk Management Policy;** • **UJ Vision, Mission and Values.**	• **Electronic Communications Act 36 of 2005;** • **Electronic Communications and Transactions Act 25 of 2002 (ECTA);** • **The Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002;** • **Protection of Personal Information Act 4 of 2013 (POPI);** • **Higher Education Act 101 of 1997;** • **The Constitution of the Republic of South Africa of 1996**
Stakeholders affected by this document (units and divisions who should be familiar with it):	• **Council Members;** • **All University Employees;** • **Student Representative Council;** • **Students;** • **All stakeholders;** • **All persons (internal or external) who make use of UJ and other social media platforms.**
Website Address:	www.uj.ac.za

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") System(s) ("ICTS") owned or leased by the University ("UJ's ICTS") extensively for purposes of electronic communication. Such communication is often the primary communication and awareness method within the University. 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 purposes of communication. Without effective control of the access to and use of its ICTS, the University's risks for exposure to deliberate or accidental misuse of its facilities increase, and sensitive information become vulnerable for disclosure to unauthorised parties (like hackers or dishonest employees). Information can also be corrupted or deleted without record. By virtue of the Electronic Communications Policy ("the Policy"), the University provides a uniform framework to manage the risks associated with communication by way of its ICTS, and to guide Stakeholders of the University, as to what constitutes fair use of the ICTS for communication as well as the responsibilities and accountabilities of the Stakeholders in that regard. Since devices such as desktop computers and mobile devices (*eg* laptops, notebooks, tablets and smart phones) can form part of, and are used to access, UJ's ICTS for purposes of communication, the Policy also deals with incidental matters relating to them.

2 PURPOSE

The purposes of this Policy are to:

2.1 make Users aware of certain risks to UJ's ICTS and to inform them of the potential consequences of not complying with the requirements of the Policy;

2.2 raise the awareness of important security issues in respect of UJ's ICTS and to assist all Users in performing their duties in a secure way;

2.3 inform and educate Users on the access to and use of UJ's ICTS for purposes of communication;

2.4 create rules for the access to and use of UJ's ICTS for purposes of communication;

2.5 provide for the interception of communications in line with legal requirements;

2.6 deal with matters incidental to the devices which are used or can be used to access UJ's ICTS for purposes of communication.

2.7 allocate roles and responsibilities to Stakeholders in respect of UJ's ICTS for purposes of communication;

2.8 ensure and maintain the values and integrity of UJ's ICTS;

2.9 provide for disciplinary action against Users who fail to comply with this 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 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 freedoms are not absolute, but restrained, amongst others, by the rights and freedoms of others;

3.1.2 to prevent or reduce the risk of the University suffering damage (including reputational damage) or incur liabilities to third parties;

3.2 a framework 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 ICTS.

5 ABBREVIATIONS AND DEFINITIONS

For the purpose of 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:

5.1	Data	The electronic representation of information in any form
5.2	Communication	Includes both a 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 be hosted 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 *User*s) 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	MEC	Management Executive Committee of the *University*
5.11	Policy	The Electronic Communications Policy
5.12	PRCC	Project and Resourcing Committee of Council
5.13	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.
5.14	Stakeholders	All *University* employees, officials, 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*
5.15	University/ UJ	University of Johannesburg
5.16	User	A *Stakeholder* to whom access is granted to use *UJ*'s *ICTS*
5.17	VC	Vice-chancellor and Principal of the *University*
5.18	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 of Health, 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 ICTS is provided for, and in connection with, the business of the University and must be used for that purpose. UJ's ICTS remains the University's property (if owned by it) or possession (if leased by it) at all times, 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, student information, employee information 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 promote employee productivity;

6.2.6 comply with the provisions of laws and regulations that govern the access, use and interception of communications;

6.2.7 investigate and take steps (including legal and disciplinary steps) in respect of unlawful or unauthorised use of its ICT and ICTS;

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

6.3 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 when they 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 retained by 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 *eg* by Yahoo, Gmail, Hotcom, etc and messages sent from such systems do not contain the UJ's e-mail legal notice.

6.4 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.

6.5 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.

6.6 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, *ie* the extent to which they can enter the public domain in their personal, as opposed to office-related, capacities.

6.7 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 ACCESS TO UJ'S ICTS

7.1 User Access Authorisation

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 Password Use

7.2.1 A unique user name is allocated to Users determined in terms of business rules.

7.2.2 All Users must be authenticated through a unique, personal, and secret password to gain access to the ICTS.

7.2.3 All Users are expected to manage their personal passwords in accordance with UJ Access control policy.

7.2.4 The safe and secure usage of UJ's ICTS is dependent on the discipline of individual Users by keeping their personal passwords safe, by terminating open sessions, by using password protected screensavers which activate after a period of inactivity, and logging out of the electronic communications facilities when any such systems are left unattended. The only exception to this is access to predefined laboratory systems using predefined shared accounts as authorised by the Executive Director of ICS

7.3 Users who are not employees

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). The aforesaid does not apply in the case of incidental use of the ICTS, *eg* the use of UJ's telephone systems by visitors to make a single call.

7.4 Impersonation

To ensure that Users are accountable and to prevent abuse of UJ's ICTS, *eg* by persons representing themselves as UJ employees or a particular UJ employee and thereby claiming authority they do not have, the following conducts is forbidden:

7.4.1 using someone else's user id and password to access the ICTS;

7.4.2 sending a fax on someone else's behalf (without their knowledge);

7.4.3 pretending to be someone else on the telephone;

7.4.4 using someone else's PIN.

8 RESPONSIBILITY OF STAKEHOLDERS

8.1 Users are personally responsible for compliance with the provisions of this Policy.

8.2 UJ's ICS Division is responsible for:

8.2.1 the technical issues related to the access to and use of UJ's ICTS for communication;

8.2.2 assisting UJ's management in intercepting communications and investigating breaches of the provisions of this Policy;

8.2.3 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;

8.2.4 scanning and filtering all electronic communications for damaging code such as viruses, and blocking them if detected;

8.2.5 implementing a decision to intercept and monitor communication as provided for by law and in terms of the Policy;

8.2.6 maintaining a UJ Information Technology Service Desk (IT Service Desk) and appoint technical employees to carry out all maintenance and support of UJ's ICTS, its components and UJ devices which are or can be connected thereto.

8.2.7 the implementation, communication, maintenance, and management of this Policy.

8.3 Users must report all ICTS related maintenance and support requests to the IT Service Desk, which will prioritise the request based upon its importance and allocate the necessary tasks to an appropriate person. Examples of such requests include:

8.3.1 suspected virus activity;

8.3.2 theft of components of the ICTS, including any computer equipment;

8.3.3 non-availability of network resources;

8.3.4 password reset requests.

8.4 The Technical Employees appointed by UJ must carry out all maintenance and support of UJ's ICTS, its components and UJ devices which are or can be connected to it. Accordingly, Users may under no circumstances:

8.4.1 attempt to repair the UJ personal computers allocated to them, or those of other Users;

8.4.2 allow unauthorised technicians to perform any support, maintenance or repair on UJ ICTS resources.

9 INTERCEPTION OF COMMUNICATION

9.1 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:

9.1.1 communications related to criminal activities;[1]

9.1.2 communications related to misconduct giving rise to disciplinary proceedings;

9.1.3 communications to establish facts related to the business of the University.[2]

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

9.2.1 by means of which a transaction is entered into in the course of its business;

9.2.2 which otherwise relates to its business; or

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

9.3 The University may only intercept an indirect communication –

9.3.1 if such interception is effected by, or with the express or implied consent of, the VC;

9.3.2 for purposes of –

(a) monitoring or keeping a record of indirect communications –

a. in order to establish the existence of facts;

---

1 such as fraud, corruption and sexual harassment.

2 for example to determine the existence, contents and interpretation of contracts.

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

c. where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or

(b) 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.

9.3.3 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.

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

9.3.5 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 a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.

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

10 OVERSIGHT MECHANISMS IN RESPECT OF INTERCEPTION

10.1 The VC will as far as is possible, seek a resolution from the MEC to intercept any indirect communication in terms of Clause 9. The MEC must consider whether there are reasons to intercept the communication without the consent of the User.

10.2 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 in terms of Clause 9 to the Projects and Risk Committee of Council, 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 inception of communication of academic members of staff. The reports must provide details of the number of Users in respect of whom communications were intercepted, the grounds on which the interceptions were undertaken, the purposes of the interceptions, 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.

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

11 ADDITIONAL MEASURES TO MINIMIZE THE IMPACT OF INTERCEPTION

11.1 Any person who actually intercepts indirect communications in terms of Clause 9 or has access to intercepted communications must treat such information as strictly confidential.

11.2 The University will not share with or disclose to third parties private and personal information obtained by intercepting indirect communication in terms of Clause 9 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.

11.3 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.

12 USE OF UJ'S ICTS FOR PURPOSES OF COMMUNICATION OTHER THAN THE BUSINESS OF THE UNIVERSITY

12.1 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:

12.1.1 if it is reasonable and not excessive;

12.1.2 if it does not consume a lot of system resources (*eg* by sending large files, or many messages via e-mail, or consuming large quantities of internet bandwidth);

12.1.3 if by an employee, it does not interfere with the performance of his or her duties as a staff member;

12.1.4 if it does not interfere with the productivity or performance of other Stakeholders or infringe upon their rights;

12.1.5 if it does not expose the University to any legal liability or cause it any damage (including reputational damage);

12.1.6 if it does not cause disruptions to the operations or resources of UJ's ICS Division;

12.1.7 if it does not violate any other provision of this Policy or any other applicable policy, guideline or rule of UJ; and

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

12.2 If UJ's ICTS is used to create, send, receive or store private or personal communication or records, then in order to protect the privacy of any such communications or records, the User should clearly mark such communication and records as "Private"; however, the Users must understand that 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 in the Policy.

13 DUTIES OF EMPLOYEES IN RESPECT OF ALL FORMS OF COMMUNICATION, INCLUDING ELECTRONIC COMMUNICATION

13.1 The contents of communication must at all times comply with the University's rules, regulations, policies and practices.

13.2 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.

13.3 An expression of a 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.

13.4 Provided that they are wrongful and there is no demonstrable need on the basis of academic freedom therefor, communications are prohibited which:

13.4.1 are or may be detrimental or injurious to the University's image, brand, reputation and relationships with others or groups;

13.4.2 are intended or may have the effect of inciting violence or advocate hatred;

13.4.3 are or may be threatening, obscene, oppressive, offensive, vulgar, profane, defamatory, discriminatory, racist, pornographic, harassing or otherwise wrongful;

13.4.4 are a violation of intellectual property rights or privacy laws;

13.4.5 bring or may bring the University or any person employed by or attending the University into disrepute;

13.4.6 indicate or gain support for any religious or political purpose.

14 PARTICULAR RULES OF CONDUCT IN RESPECT OF E-MAIL

14.1 When forwarding or replying to e-mail messages, the contents of the original message should not be altered. If the contents need to be changed, then all changes must be clearly marked as such (*i.e.* modifications, additions, deletions, removal of recipients, etc.).

14.2 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.

14.3 Users must always maintain the privacy of group members whenever the members of the group are unaware of the identities of the other members of the group, *e.g.* by utilising the Bcc facility.

14.4 The following, actions and activities are prohibited:

14.4.1 Fabricating a message and/or sender of a message;

14.4.2 Modifying the internal mail transport mechanism to forge a routing path that a message takes through the internet;

14.4.3 Knowingly sending or forwarding messages and attachments that are infected with malicious codes such as viruses, worms, trapdoors or Trojan horses (if such code is discovered, the user must cease using the system immediately and immediately report the discovery to the IT Service Desk);

14.4.4 Messages with include hyperlinks or other directions to content that breach Clause 13;

14.4.5 Participating in e-mail "chain letters" or similar activities;

14.4.6 Downloading, receiving and/or installing software applications not approved by the ICS Division which has a right to remove any unapproved software without the prior consent of the employee;

14.4.7 Knowingly burdening UJ's ICTS with data unrelated to UJ's business (*e.g.* forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server);

14.4.8 Using automatic forwarding of e-mails ("Auto Rules") to any UJ employee without such

person's consent;

14.4.9 Using automatic forwarding of e-mails ("Auto Rules") to any non-UJ employee;

14.4.10 The creation, sending or forwarding of unsolicited mail (spam);

14.4.11 The creation, sending or forwarding of marketing information or advertising material unrelated to UJ's business;

14.4.12 Downloading, reproducing, sharing, retaining and/or creating records that contain music, images, sound or video if such exceeds reasonable personal use and should the ICS Division re-images a computer it has no duty to back up or replace such files;

14.4.13 Any actions that knowingly prevent other Users from using and accessing UJ's ICTS;

14.4.14 Taking any of the steps or actions criminalised and detailed in Chapter XIII of the Electronic Communications and Transactions Act 25 of 2002 or any other legislation, including, but not limited to, hacking, gaining or attempting to gain access to restricted resources either inside or outside of the University's computer network or developing, downloading and using any technology that may circumvent ICS security measures;

14.4.15 Any unreasonable or disruptive practices to UJ on, through or with ICT and ICTS;

14.4.16 Sending, replying to or forwarding e-mail messages or other electronic Communications which misrepresent or hide the identity of the sender or represent the sender as someone else;

14.4.17 Encrypt messages, attachments or records that prejudice UJ;

14.4.18 Accessing any other person's inbox or other e-mail folders or send any email purporting to come from another person without explicit prior written authorisation from that person or by means of Outlook delegates;

14.4.19 Using or accessing UJ's ICT or ICTS to commit fraud or any other criminal offence(s).

14.5 Users should take care when receiving emails with file attachments, even if that email appears to come from a known source, since a virus embedded in an email message cannot only damage the recipient's data, but can also spread throughout UJ's network.

15 CONFIDENTIAL COMMUNICATION

UJ's electronic communications facilities are not automatically protected against disclosure to unauthorised individuals. Therefore:

15.1 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 SMS or telephonically. Encryption and the use of VPN can also be considered;

15.2 when faxing information deemed confidential and/or proprietary to UJ, a User must ensure that the recipient is "standing-by" to ensure that the fax does not fall into the wrong hands;

15.3 when communicating via a voice network (*eg* telephone) and confidentiality is at stake, a User must verify the identity of the individual (through asking security question) and ensure that the individual is authorised to receive any information deemed confidential and/or proprietary to UJ;

15.4 when remote access to sensitive and confidential information stored on UJ servers 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.

16 PROTECTION OF DEVICES CONTAINING RECORDS OF COMMUNICATION

16.1 Users must take reasonable and appropriate measures to protect the components of UJ's ICTS (including devices providing access to the ICTS, like computers) used by them against accidental or malicious destruction, damage, or unlawful modification. Where possible, all workstations, laptops and 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.

16.2 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 logged out from when any such systems are left unattended, and encryption tools or techniques used and authorised by UJ's ICS department. 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.

16.3 Mobile devices (*e.g.* laptops, tablets and cell phones) 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 than may be required, the following examples are provided:

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

16.3.2 Ensuring that UJ devices are not used by non-UJ personnel;

16.3.3 Being careful when devices which 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;

16.3.4 Ensuring that confidential information is not inadvertently viewed by third parties (*e.g.* when using laptops on public transport or in airport lounges);

16.3.5 Ensuring that confidential information stored on mobile devices is password protected or encrypted;

16.3.6 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

cellular phones) is regularly backed up;

16.3.7 Guarding against unintentional disclosure of 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 or using public fax facilities and phones.

16.3.8 Using suitable techniques (*e.g.* though encryption mechanisms approved by the ICS Division) to protect University information, stored on mobile devices (such as laptops, personal organisers, USB memory sticks and cellular phones) and home computers from disclosure.

16.3.9 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.

16.3.10 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.

16.4 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.

16.5 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), 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 time period.

16.6 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 UJ from them since it is not the intention of UJ to retain such information, particularly private and personal information of a User. UJ accepts no responsibility with regard 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 wiped clean 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. Clauses 10 and 11 of the Policy (save for 11.2 with the necessary amendments) are not applicable to the provisions of this subclause (Clause 16.6).

17 SECURITY OF ICTS WHEN CONNECTING DEVICES TO IT

Certain software installed on desktop computers and laptops can cause damage to the ICTS and other Users when connected to the UJ ICTS (*e.g.* when it contains viruses or constitutes malware), hence the University generally installs the software on such UJ devices allocated to Users to perform their duties safely and securely. For this and other reasons the following provisions apply to secure the UJ ICTS:

17.1 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 ED of the ICS Division. Modifying, revising, adapting, translating, reverse-engineering or disassembling software is prohibited.

17.2 No unlicensed (pirated) software or data may be uploaded to UJ devices. The IT Helpline must be contacted if in doubt about the copyright regarding software which can be downloaded from the internet.

17.3 Virus management software installed on UJ devices must be kept up to date by connecting the devices to the ICTS regularly. Where privately owned devices are used to store UJ records, users must ensure that the virus management software provided with those devices is up to date.

17.4 A list of approved software that may be installed on UJ devices is updated on a regular basis and published on the UJ Intranet. If a User believes that a particular software product, whether freeware, shareware or proprietary software, would assist in furtherance of UJ's business, then a motivation should be sent to the ED of the ICS Division.

17.5 Users are prohibited from installing or playing games on UJ devices.

17.6 Network configurations on UJ supplied devices may not be modified; these include changes to e-mail, internet, email, dialup, and network protocols and settings (such as IP settings).

17.7 When connected to the ICTS (UJ network), Users may not establish simultaneous connections using any non-UJ approved method to connect to personal Internet Service Providers, external networks or third parties, whilst simultaneously connected to UJ network. Simultaneous network connectivity is strictly forbidden without prior, written authorisation from the ED of ICS

18 GENERAL

18.1 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 overloading of UJ's ICTS.

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

The University 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 *eg* 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).

19 DUTY TO DISCLOSE AND REPORT

Users must report known or suspected violation of the provisions of this Policy to the UJ ICS Division or their line manager.

20 POLICY INFRINGEMENT

20.1 Breaches of the Policy are dealt with on a case-by-case basis and according to the severity of the breach.

20.2 Under appropriate circumstances breaches of the Policy may be referred to the University's Human Resource Management Division or Student Judicial Affairs Division for disciplinary action. Depending on the severity of the breach of Policy, disciplinary action may result in dismissal (in the case of employees) or expulsion (in the case of students).

21 DEVIATION FROM THE POLICY

The Executive Director of the ICS Division or the MEC must approve any deviations from the Policy, depending on the nature of the deviation sought.

22 INTERPRETATION AND COMMENCEMENT

22.1 Any reference to the singular includes the plural and vice versa. A reference to gender includes all genders.

22.2 Should any statute or statutory provision to which the Policy refers be amended or replaced by another statute, any reference in the Policy to that statute or statutory provision will be interpreted to refer to the amended statute or statutory provision, or to the statute or statutory provision which replaces the statute or statutory provision to which the Policy refers.

22.3 If any provision of the Policy is or becomes invalid or unenforceable by virtue of law, such provision shall be divisible and be regarded as *pro non scripto* and the remainder of the Policy shall be regarded as valid and enforceable.

22.4 If any definition contains a substantive provision, notwithstanding that it is only in the definition (or such other clause) effect shall be given to it as if it were a substantive provision in the body of the Policy.

22.5 The use of the word "including" or other grammatical forms thereof followed by specific examples shall not be construed as limiting the meaning of the general wording preceding it and the *eiusdem generis* rule shall not be applied in the interpretation of such general wording or such specific examples.

22.6 No provision of the Policy referring to wrongfulness or other grammatical form thereof shall be interpreted to determine the onus of proof in respect of wrongfulness. Whether the University carries the onus to prove wrongfulness, or someone who is alleged to have breached the Policy is required to disprove wrongfulness (for example, exclude wrongfulness by proving a ground of justification where appropriate, for example, by relying on the defence that the publication was true and in the public interest, or that the publication constituted fair comment in the case of defamation) is determined by law.

22.7 The Policy does not seek to fully codify the issues to which it refers and shall not be interpreted to (in any way) amount to a waiver, or prejudice or limit the University's rights and remedies against Stakeholders in terms of the Law and the codes of conduct applicable to Stakeholders.

22.8 The Policy or any amendment thereof will come into operation when approved by the appropriate structures of the University, at which time it will replace the Electronic Communications Policy of 2009.