RAJARATA UNIVERSITY OF SRI LANKA

SENATE MEETING

AGENDA & MINUTES FOR THE

MEETING NO. 225

ශ්‍රී ලංකා රජරට විශ්වවිද්‍යාලය
ஸ்ரீ லங்கா ரஜரட பல்கலைக்கழகம்
Rajarata University of Sri Lanka

මිහින්තලේ
மிகின்தலே
Mihintale

ශ්‍රී ලංකා
ஸ்ரீ லங்கா
Sri Lanka

දූරකථන(සාමාන්‍ය) தொலைபேசி Telephone(General): 025-2266643, 2266645, 226664x6, 2266650
Registrar: 025-2266511

ෆැක්ස් பெக்ஸ் Fax: 025-2266511, 2266512
Deputy Registrar (Examinations & Academic) – Tel: 025 - 2266780

ඔබේ අංකය
உமது இலக்கம்
Your Ref.

මගේ අංකය
எனது இலக்கம்
My Ref. RJT/EX/Senate/2020

දිනය திகதி Date: 18th February 2020

Dear Sir/ Madam,

225th Meeting of the Senate – Rajarata University of Sri Lanka.

The 225th Meeting of the Senate will be held at *1.30p.m.* on *Thursday 27th February 2020* at the Main Auditorium of the Rajarata University of Sri Lanka, Mihintale.

The Agenda, connected papers and the Minutes of the 224th Senate Meeting **will be e-mailed on 24th February 2020** to your personal email account.

Your presence at this meeting will be highly appreciated.

Yours faithfully,

Deputy Registrar/ Examinations & Academic

Travelling program
19 sts. prof.
Dr. Buddi-Tech
Japan empan
visit. Apr 2.

(10)

05-100

[Senate Memo No. 225.05.23]

Rajarata University of Sri Lanka

University Information Technology Usage Policy

On the recommendation of the Senate, the Council of the Rajarata University of Sri Lanka, as the governing authority of the Rajarata University of Sri Lanka, by resolution adopts the following policy.

Dated: 11.02.2020

Last amended: Not Applicable

Signature: Signed

Position: Vice Chancellor, Rajarata University of Sri Lanka

This Policy may be referred to as University information Technology Policy No. 01/2020

Contents

05-101

1. Background

The University envisages to become a centre of excellence in higher education by creating a highly conducive environment for teaching, learning, and research in diversified disciplines as well as for efficient administration. For this purpose, it is in the process of developing a state-of-the-art Information Technology (IT) infrastructure and upgrading the human and physical resources to be on par with the infrastructure in order to facilitate seamless and unified communication, ease of access to information, and resource sharing. Hence, many aspects of teaching, learning, research, and administration are becoming more and more dependent upon the availability, integrity, and confidentiality of digitized information and (IT) based services. The reliability and security of the IT infrastructure need to be enhanced and adequacy of services provided need to be constantly maintained and monitored. This policy document is intended to provide guidance to the usage of IT resources in the University and the best practices applicable to such usages.

This policy and any relevant guidelines developed subsequently shall apply to:

- students of the University, internal or external they may be, who use the IT infrastructure, services, an / or devices provided by the University,
- staff of the university, including, The Vice-chancellor, Deans, Heads of Departments / Units / Administrative divisions who use the IT infrastructure and related services for their duty related or other activities
- guests of the University who use the IT infrastructure, services, and devices provided by the university
- any IT related service, information, or a tool provided by the University for the purpose of teaching, learning, research, and administration as envisioned by the University.

Objectives of this document is to:

- ensure that all applicable resources such as computer systems, information assets, and infrastructure will be available to everybody within the University without any prejudice or discrimination
- increase awareness of the Fair User Policy (FUP) applicable to the use of IT infrastructure and related services
- increase awareness and understanding of the requirements of IT security among both employees and students as well as any third party who access IT systems of the University
- ensure that the availability, integrity, and confidentiality of all the University's computer systems, information assets, and infrastructure will be protected from threats whether internal, external, deliberate or accidental
- ensure that adequate and substantive human resources are recruited and developed within the University to guarantee seamless operation of the infrastructure, services, and the devices
- provisioning for the development of codes of ethics and manual of procedures to impartially handle any violation of this policy and any subsequent guidelines.

2. Pretext

The University endeavours to deliver a robust and fit for purpose IT infrastructure to support its strategic mission, objectives and priorities. Users (students, staff and other parties who are accessing the IT resources of the University) are encouraged to use the computer systems to the fullest extent to support teaching, learning, research, and other related University work. They are further encouraged to bring their own devices

and use them in conjunction with University supplied facilities. However, all IT users have responsibilities which must be honoured, and will be held individually responsible for any and all activities undertaken by them. They are also required to honour the equal right of access of all users and the FUP.

3. Governance

The Council of Rajarata University of Sri Lanka will be the apex governing body for the policies and any subsequent guidelines of this policy. However, the Council, upon recommendations from the Deans of the Faculties, and the Director of the IT Centre, may assign the responsibility to a suitable entity such as a steering committee, IT committee or IT Centre. Nevertheless, all staff, especially, The Vice-chancellor, Deans, Heads of Departments / Units / Administrative divisions are responsible for upholding the policies and any subsequent guidelines of this policy.

4. General Conditions

4.1. This set of policies has been approved by the Council of Rajarata University of Sri Lanka and forms part of the policies and procedures of the University. It is applicable to all users of IT facilities provided by the University.

4.2. This Policy and any associated guidelines shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any changes in technology, the law, or University policy.

4.3. University IT resources are provided primarily to facilitate users' essential work related to teaching, learning, research, or other related University work. Priority of using University IT resources must always be granted to those needing facilities for academic or other essential work. Uses for non-work-related purposes, such as personal electronic mail or recreational use of the World Wide Web including social networking sites, are understood to enhance the overall experience of an employee or student, but are not considered an absolute right.

4.4. No use of any IT facility should bring the University into disrepute, in any way.

4.5. University e-mail addresses and associated University e-mail systems must be used for all official University activities. All staff and students of the University must regularly read their University e-mail.

4.6. Use of IT facilities for commercial work, or for outside bodies, is strictly prohibited unless an explicit permission from the relevant authorities is obtained.

4.7. Management and integrity of central computing servers, systems, core network switches, backup systems, and the overall network infrastructure interconnecting these systems is the responsibility of the IT Centre or any other entity as decided by the Council.

4.8. University shall make sure that an adequate number of staff with suitable qualifications are employed at the IT Centre, as well as in the Faculties / Administrative Divisions, as deemed necessary by the usage. The staff shall have up-to-date knowledge on various services offered and a high-level of troubleshooting ability.

4.9. A user shall never attempt either to damage, or to compromise the security of, the internal systems of the University.

4.10. A formal complaint should be made to the Director/ IT Centre if users suspect that the confidentiality or privacy of their personal information has been violated without authorization. The IT Centre should investigate such complaints and inform the outcome and report to the Vice Chancellor if the University's rules and regulations are found to be violated.

4.11. All users have a responsibility to report promptly (to the IT Centre) any incidents which may have an IT security implication for the University.

4.12. Specialist advice on information security shall be made available throughout the University by the IT Centre.

4.13. The University will strive to protect the privacy and confidentiality of any user information held within its IT infrastructure. However, the University is not liable for any breach of privacy and/ or confidentiality, and accidental or intentional disclosure of such information.

4.14. Every effort shall be taken to safeguard user data and information of users residing in the University's IT system. However, the University is not liable for loss of such data and information.

5. User Administration

5.1. Some IT facilities provided by the University are unrestricted and may be used by anybody having a suitable device. Nevertheless, The University does reserve the right to discontinue these services at any time, or to disconnect people or devices if they (or their device) are causing disruption to the security and efficiency of the systems. Use of all other facilities either require a user to have a username and a password, or the device connected to have its hardware addresses to be registered.

5.2. The usernames and passwords to access different services may be issued by the relevant department, section, or administrative branch. Registering of the devices is primarily done by the IT Centre, however, any relevant department, section, or an administrative branch also may do so provided that the service is administered by them.

5.3. Once the University has established fully operational identity service and unified communication system, all the usernames and passwords, along with an official e-mail address will be provided by IT Centre to all users. At this point, registering of the hardware devices will also be a responsibility of the IT Centre.

5.4. In order to obtain permission and/ or credentials to access IT resources of the University, a prospective user shall make a written request either in the form of an application (whenever available), or a letter with the recommendation(s) of the Heads of Departments / Units / Administrative Divisions and relevant Dean of the Faculty or Registrar. This application shall serve as the applicant's agreement to abide by the rules and regulations of the University and the guidelines defined in this policy. IT Centre will issue the permission and/ or credentials if they are satisfied that the applicant fulfils all the requirements to be accepted as a user.

5.5. All individually allocated items such as usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. Users shall not use or acquire the credentials of others, or attempt to impersonate them, or reveal their credentials to others.

5.6. No one may use, or attempt to use, ICT resources allocated to another person, whenever such resources are allocated on a quota basis, except when explicitly authorized by the provider of those resources under exceptional circumstances.

5.7. All users must correctly identify themselves at all times. A user must not impersonate another, withhold their identity or tamper with audit trails.

5.8. Passwords are an important part of system security. For most systems, the system itself will show and enforce the minimum quality rules that are required of a password. If not, the commonly accepted guidelines for a strong password (a combination of uppercase and lowercase letters, numbers and special characters with at least two characters from each category to form a minimum of eight characters

05-104

in total) must be used. Whenever the user is allowed to change the password, the user shall never use a commonly accepted "weak" password.

5.9. Any security breach due to the use of a "weak" password may result in disciplinary actions, that may be defined subsequently, against the user.

5.10. The IT resources provided by the University may be directly or indirectly linked with IT resources of other institutions. In such cases, the use of the University's credentials to gain unauthorized access to the facilities of any other organization is prohibited.

6. Privacy of Users

6.1. The staff of the IT Centre, or any academic or administrative staff members authorised by the University, who have appropriate privileges, and have the ability, may be occasionally required to access all files, including electronic mail files, stored on any computer which is attached to the University IT resources, may it be provided by the University, or a personal device. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of users.

6.2. However, in case of accidental or unintentional disclosure of any such material, which may cause any damage to the privacy or reputation of the user, the University or the staff involved may not be held responsible.

6.3. The University fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit. Reasons for such monitoring may include the need to:

- 6.3.1. ensure operational effectiveness of services,
- 6.3.2. prevent a breach of the law, this policy, or other University policy,
- 6.3.3. investigate a suspected breach of the law, this policy, or other University policy,
- 6.3.4. monitor standards.

6.4. Access to staff files, including electronic mail files, will not normally be given to another member of staff unless explicitly authorized by a Dean of the Faculty, Head of the Department, Head of the Centre or Unit, or Officer in charge. Such access will normally only be granted in the following circumstances:

- 6.4.1. where the staff requires access to e-mail messages or files of an individual, which are records of a university activity, and the individual is unable (e.g. through absence) to provide them,
- 6.4.2. where a breach of the law or a serious breach of this or another University policy is suspected,
- 6.4.3. when a documented and lawful request from a law enforcement agency has been received.

6.5. The University sees student privacy as desirable but not as an absolute right. Systems staff are authorized to release the contents of a student's files, including electronic mail files under following circumstances:

- 6.5.1. when a breach of the law or of this policy is suspected,
- 6.5.2. when a documented and lawful request from a law enforcement agency has been received,
- 6.5.3. when required by any member of staff who has a direct academic work-based reason.

6.6. The University advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorized persons.

6.7. After a student or member of staff leaves the University, files which are left behind on any computer system owned by the University, including servers, and including electronic mail files, will be considered to be the property of the University.

6.8. When leaving the University, staff should make arrangements to transfer to colleagues any e-mail or other computer-based information including access credentials of secured systems held under their personal account where appropriate, as access authorizations are terminated within 60 days of their departure.

7. Use of Resources

7.1. The following policies apply for any use of IT resources provided by the University, may it be utilising the hardware resources provided by the University or personal devices.

7.2. End-user Devices

7.2.1. All end-user devices, such as computers, laptops, tablets, handhelds, telephones, smartphones and any other similar devices must be adequately protected all the time so that they are not physically damaged. In case of a physical damage to a device, the user is liable to fully compensate the damage.

7.2.2. The University shall strive to provide licensed software, including operating systems, for all end-user devices provided by the University. In some instances, the University may provide licensed software to be used in personal devices as well.

7.2.3. In a situation where a licenced software is not provided, users are encouraged to use free and open-source software in their devices.

7.2.4. The relevant user may be held responsible for any consequence of the use of any un-licensed commercial software which is not endorsed by the University in an end-user device provided by the University.

7.2.5. The University may provide appropriate malware protection tools for the devices provided. However, if any device is not provided with such tools, the user has to make sure that device is maintained malware-free by taking appropriate measures. In cases where such malware protection tools are provided, the user shall not tamper with it, leaving the device vulnerable to malware attacks.

7.3. Networks and Infrastructure

7.3.1. Wired and wireless networks, servers, and other infrastructure facilities, provided by the University to ensure seamless connectivity across its premises, are intended to be used for teaching, learning, research and other University work related activities.

7.3.2. The use of such facilities for entertainment purposes and social networking activities, is not prohibited, however, may be restricted as deemed necessary by the University.

7.3.3. The network and all related equipment and services provided by the University shall be maintained by suitably authorized and qualified staff to oversee its day to day running and to preserve its security and integrity. All network management staff shall be qualified and skilled for the purpose and be given relevant training in IT design, troubleshooting, and security issues.

7.3.4. The network must be designed and configured to deliver high performance and reliability to meet the intended purposes, whilst providing a high degree of access control and a range of privilege restrictions. The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorized intrusion.

7.3.5. Adequate measures must be taken to ensure 24/7 operation of the network and related services provided by the University. Appropriately configured power supplies, including uninterruptible power supplies, and where necessary, generators, must be provided to ensure continuous availability of these services throughout the University.

7.3.6. The University intends to establish a secure wireless network with proper authentication and authorization procedures. For this purpose, a secure network access controller shall be installed which ensures creation of segregated security zones, with routing and access controls operating between the zones, to reduce the possibility of internal or external users gaining unauthorized access to systems.

7.3.7. Systems with particularly high security vulnerabilities shall be protected both from internal and external access. All other systems will be protected from external access by default. Appropriately configured firewalls shall be used to protect the network supporting the University's systems.

7.3.8. Access to the resources on the network must be strictly controlled to prevent unauthorized access by access control procedures that provide adequate safeguards through robust identification and authentication techniques. Remote access to resources on the network will be made available only through authorized entry points, normally through the site firewall. Remote access to non-public resources will be subject to authentication and other security mechanisms.

7.3.9. Each user shall be allocated to a particular security zone to control security breaches of the network system. There can be certain zones in which all or some users are allowed. Special segregations will be applied to control the usage of network and related services by authorized users in unauthorized zones.

7.3.10. Faculties/ departments/ units/ centres/ administrative branches should refrain from creating their own Wi-Fi networks other than for research purposes without informing and explicit written permission from the Director of IT Centre. Any access points installed should be secure and able to authenticate individual users and optionally connected to the secure access controller maintained at the IT Centre.

7.3.11. All users are responsible for the protection of network, and no one shall try to access resources that are intended to a different privilege level. Moving, removing, or damaging hardware components or tampering with the software or security systems of the University network is strictly prohibited. Any user who is found to be guilty of committing any of these offences will be punished. The procedures for disciplinary actions and the relevant punishments shall be developed by the University.

7.4. Information

7.4.1. An inventory will be maintained of all the University's major information assets and the ownership of each asset will be clearly stated. Within the information inventory, each information asset will be classified according to sensitivity. When permanently disposing of

equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted.

7.4.2. Software and/ or information provided by the University may only be used as part of the user's duties as an employee or student of the University or for educational purposes. The user must abide by all the licensing agreements for software entered into by the University with other parties, noting that the right to use any such software and/ or information outside the University will cease when an individual leaves the University.

7.4.3. All information held in the IT systems provided by the University shall be protected from unauthorised access and / or disclosure, accidental or deliberate deletion, unauthorised modification and fabrication.

7.4.4. Backup of the University's information assets and the ability to recover them is an important priority. Respective 'owners' of systems are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the operational needs of the University. In case of removable backup media, they must be stored in an area that is remote from the physical system that has been backed up. If the backup is done on a separate server, the server must be located in a different building than the source system. In the case of critical information systems where 24/7 service is required, consideration must be given to deploying fault tolerant equipment.

7.4.5. All information included in the University website must be formally endorsed by the relevant authority. Any information, including news, that should be included in the university website must be directed to the Director of the IT Centre, or any such entity that is responsible for maintaining the University website through the Vice-chancellor, Dean, Head of Departments / Units / Administrative division relevant.

7.5. Communications

7.5.1. Users should be conscious of all possible security attacks and consider how emails sent might be used by others. Similarly, users should not necessarily trust what is received in an email - in particular, users must never respond to an email request to give a username and/ or password.

7.5.2. Email must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure confidentiality: that it is correctly addressed, intended recipients are authorized to receive it, and passwords are used to protect attached documents where required.

7.5.3. Users should consider the security implications of any information they put on the University's Website, and the University reserves the right to remove any material which it deems inappropriate, illegal or offensive.

7.5.4. Users should not in any way use any areas of the University Website for commercial purposes, or to publish material which undermines IT security provided by the University.

7.5.5. Email addresses and fax telephone numbers should be checked carefully prior to transmission, especially where the information content is confidential or sensitive, or where the disclosure of email addresses or other contact information to the recipients is a possibility. The attachment of data files to an email is only permitted after confirming the confidentiality

classification of the information being sent and checking that the document will have been scanned for the possibility of a virus or other malicious code.

7.5.6. Information received via email must be treated with care due to its inherent information security risks. File attachments will be automatically scanned for possible viruses or other malicious code.

7.5.7. Confidentiality of all sensitive information received should be highly observed. Sensitive information obtained for temporary use should be properly destroyed after use.

7.5.8. The University may provide virtual private network access for the users to seamlessly access information and services provided for internal users. Use of such services, including unified communications, may be prohibited by national level and international regulations. Users are held responsible for any such breaches of law by using these services.

7.5.9. The management of Internet connectivity is intended to

- promote a harmonious workplace,
- manage the costs of the provision of the internet service,
- ensure the University complies with relevant legislation at the national level, and
- prevent the University from becoming the subject of an external investigation.

7.5.10. All users, including guests, are provided with facilities and equipment, including the provision to use end-user devices, to allow them to access the internet for legitimate University work, study, and research related activities. The access quota available to each user will be determined by the University to be sufficient for the needs of the relevant user.

7.5.11. A reasonable amount of non-work-related activity is acceptable; however, this must not interfere with work related activities.

7.5.12. If a website containing inappropriate or objectionable material is inadvertently opened the website must be immediately exited.

7.5.13. Access to the internet is open, subject to the following restrictions:

- Access to objectionable material is prohibited. Where the accessing of objectionable material is required for research purposes, the formal written approval of the relevant Ethics Review Committee must be obtained.
- Access to inappropriate material is prohibited. Where such material is required to be accessed, the accessing individual must ensure that such content is not observable by others. Such material may cause offense to others, who may make a complaint which will result in an investigation and consequently in a disciplinary action.
- All peer-to-peer usage must be for legitimate University business only.
- All use, sharing, or reuse of licenced and/or copyrighted materials must be in accordance with the national copyright policy.

8. Acceptable and Unacceptable Usage

8.1. Acceptable uses may include:

8.1.1. use of ICT resources for teaching, learning, research, administration or any other official activities of the University.

8.1.2. personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others.

8.1.3. advertising via electronic notice boards/ forums, intended for teaching, learning, research, administration or any other official activities of the University, or via other University approved mechanisms. However, such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

8.1.4. use for commercial purposes in case of start-ups endorsed by the University as a part of entrepreneurship development of students.

8.2. Unacceptable use of University computers and network resources may be summarized as:

8.2.1. the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognized research or teaching that is permitted under university regulations and common law; propagation will normally be considered to be a much more serious offence.

8.2.2. intellectual property rights infringement, including copyright, trademark, patent, design and moral rights, including use internal to the University.

8.2.3. causing annoyance, inconvenience or needless anxiety to others.

8.2.4. defamation, however, genuine scholarly criticism is permitted.

8.2.5. unsolicited advertising, often referred to as "spamming".

8.2.6. sending e-mails that purport to come from an individual other than the person actually sending the message using a masquerading mechanism.

8.2.7. attempts to break into or damage computer systems or data held thereon.

8.2.8. actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software.

8.2.9. attempts to access or actions intended to facilitate access to computers for which the individual is not authorized.

8.2.10. using the University network for unauthenticated access.

8.2.11. attempts to disrupt services of IT systems including e mail, web based and other related services.

8.3. These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

8.3.1. the downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid license, or other valid permission from the copyright holder

8.3.2. the publication on external websites of unauthorized recordings or photos.

8.3.3. the distribution or storage by any means of pirated software

8.3.4. connecting an unauthorized device to the University network.

8.3.5. circumvention of Network Access Control.

8.3.6. monitoring or interception of network traffic, without explicit permission.

8.3.7. probing for the security weaknesses of systems by methods such as port-scanning, without permission.

8.3.8. associating any device to network Access Points, including wireless, for which you are not authorized.

8.3.9. non-work and non-study related activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs.

8.3.10. excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action.

8.3.11. use of University owned computer laboratories unnecessarily, especially where such activities interfere with others' legitimate use of IT services.

8.3.12. opening an unsolicited e-mail attachment, especially if not work or study-related.

8.3.13. the deliberate viewing and/or printing of pornographic images.

8.3.14. the passing on of electronic chain mail causing problems for other users.

8.3.15. posting of defamatory comments about staff or students on social networking sites.

8.3.16. the creation of web-based content, portraying official University activities without express permission or responsibility.

8.3.17. the use of University mass mailing lists for non-work purposes.

8.3.18. the use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.

8.3.19. the copying of other people's Web site, or other, material without the express permission of the copyright holder.

8.3.20. the use of peer-to-peer and related applications within the University. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, etc.

8.3.21. Plagiarism in any form.

9. Monitoring and Enforcement

9.1. Computing equipment, network infrastructure and access to the internet are provided by the University to staff and students for work, study, and research purposes and not for personal use. If a user uses her / his University supplied computer or other digital device for personal use, she/ he will be subjected to University monitoring.

9.2. The University monitors the usage and content of University computers, servers and associated devices. Monitoring is an ongoing activity of the IT Centre which uses software tools to check the digital characteristics of files that may signal compliance or cyber security risks. Monitoring can occur at any time, and without prior notice to any staff member or student using the computing resources of the University. When a problem file is found, IT Centre may initiate a further investigation and take action to resolve the risk in accordance with the procedures defined in relevant University policies.

9.3. The University may, with the prior approval of the Registrar or the Vice-Chancellor, upon receiving substantial evidence of any breach of this policy or any other University policy or national or international laws and regulations, and subsequent to a preliminary investigation, examine in detail the content, of any computer which has been provided by the University, or which is connected to its networks, at any time, and without prior notice to the staff member or student using the computer. This includes accessing emails or other electronic communications, and any data stored on or processed through the University networks. However, the University shall use any such monitored or revealed material only for the purpose of decisions regarding disciplinary actions against the relevant personnel.

9.4. IT Centre will advise the relevant Dean of the Faculty, Head of the Department, Head of the Centre or Unit, or Officer in charge as appropriate of any suspected breaches of this policy. Any concerns will be investigated in accordance with the relevant University policies and procedures. Breaches of this policy may be viewed as serious misconduct which could result in disciplinary action being taken.

Document History and Version Control

Version No.	Action	Approval Authority	Effective Date
1.00	*Document development*	*Senate*	*February 2020*