Ramdeobaba University

Nagpur -440013

IT POLICY

2025

Avinash J. Agrawal

1		**Introduction**
		The Ramdeobaba University (RBU) provides computing equipment and access to the internet to enable staff to carry out their work for the RBU. The aim of this policy is to define what the RBU considers appropriate usage of the IT infrastructure and internet and how access to the internet will be managed and monitored. The management of IT infrastructure and internet access as noted in this policy and the intended is to promote a harmonious workplace, to make optimum usage of facility, to improve the quality of education, to manage the costs of the provision of the IT and internet service, to ensure the RBU complies with relevant National / International legislation. The purpose of the policy is to • provide guidance on the use of the RBU computing and internet resources • ensure that approved users are aware of the legal consequences attached to inappropriate use of these computing and internet facilities • establish a framework within which all approved users can self-regulate their use of the resources • advise users that their usage of the Internet will be monitored and, in some cases, recorded and • set out the actions that the RBU will take, in support of the Information Technology Services (ITS) regulatory framework, to investigate complaints received from both internal and external sources, about any unacceptable use of the Internet that involves the use of IT Resources. In applying this policy, the RBU will have regard to the need to ensure that users have freedom within the law to question and test received wisdom and to put forward new ideas and controversial or unpopular opinions. The RBU will also have regard to the need to ensure that such freedom is exercised in a way which does not unduly infringe on the legitimate rights and interests of others.
2		**Objective**
		IT infrastructure and Internet access are tools that are provided for authorized use by the members of the RBU and users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. The objective of this policy is to ensure proper access and usage of RBU IT/internet facilities and prevent their misuse by the users. The IT infrastructure and internet users are expected to be familiar with and to comply with this policy.

3		**Scope**
		This policy governs the usage of IT infrastructure and internet from an end user's perspective. This policy is applicable to all faculty members, staff, students, research scholars, alumni and people from industry who access, use, handle or manage the IT/internet facilities. All persons mentioned above are referred to herein as "users".
4		**Mandatory References**
		The IT policy shall confirm IT Act 2023 as amended from time to time.
5		**Definitions**
	a	**Computer** - includes any electronic device provided by the RBU, or connected to its networks, which is capable of accessing the internet.
	b	**Internet usage** - for the purpose of this policy internet usage includes accessing websites, email, peer to peer networking and data sharing and "internet" has a corresponding meaning.
	c.	**Firewall** – a network security system, either hardware or software-based, that controls incoming and outgoing network traffic based on a set of rules.
	d.	**Website** – a destination endpoint on the internet; a URL or an IP address.
	e.	**Inappropriate material** - is material which could reasonably be described as unsuitable or offensive having regard to the nature of the particular workplace as determined by the CNC Team.
	f.	**Objectionable material** – Material that it is illegal to view or possess, such as child pornography and depictions of bestiality. Accessing such material is an offence punishable at law with serious penalties, including, for certain offences, imprisonment.

	g	**Infringing file sharing** – Refers to the sharing of music, movies, and other copyright or licensed material using peer to peer file sharing mechanisms, for example, 'torrenting'.
	h.	**Authorized Use** - Authorized Use Resources is use that the RBU determines, in its sole and exclusive discretion, is consistent with the education, research, and service mission of the RBU, consistent with effective departmental or institutional operations, and consistent with this policy.
	i.	**Authorized Users** - The RBU may control access to Resources in accordance with RBU policies and procedures limiting use to Authorized Users. Authorized Users may include: • Current faculty members, staff, students and alumni of the RBU • Research scholars and people from industry
	j.	**Resources** - Resources means the RBU's computing, network and information technology resources, including without limitation all data and information in electronic format or any hardware or software that makes possible, in the broadest possible sense, the processing, transmission, storage or use of such information. As an example, included in this definition are • Access identity accounts and login processes • Communications devices • Computers • Data • Databases • Digital images • Digitized information • Electronic mail • Messaging • Network devices and wireless access points • Servers • Firewall • Software • Storage devices • Websites

		• Blogs and public information services • Workstations • Local Area Network (LAN). • Google Drive • Single mode/Multimode fibre optical cable • 1Gb and 10Gb Network Capacity • Biometric system • Digital Library for research work
	k.	**Breach** - An information security incident that involves users not using Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner.
	l.	**Copyrighted content** - Material for which the copyright for the content is held by a third party other than RBU. e.g. music, computer software, films, video.
	m.	**P2P Application** – It is software running on device to provide the communications of file sharing capabilities between peers. This software is usually downloaded from the Internet and includes but not limited to applications such as Kaaza, Torrent and Limewire.
	n.	The Central Networking and Computing facility (CNC) is responsible for: 1. establishing Internet security policies and standards 2. providing technical guidance on computer security 3. ensuring there is an appropriate policy and procedure in place to respond to virus infestations, hacker intrusions and similar events 4. monitoring compliance with Internet security requirements, including hardware, software and data safeguards 5. providing administrative support and technical guidance on matters related to Internet security 6. periodically conducting risk assessments on information systems to determine both risks and vulnerabilities 7. checking that appropriate security measures are implemented on systems in a manner consistent with the level of information sensitivity 8. checking user access controls are defined in a manner consistent with the need-to-know

	o.	**Users** of RBU are responsible for: 1. ensuring that they comply with this policy and practices pertaining to Internet security at all times 2. not permitting any unauthorized individual to obtain access to RBU Internet connections 3. not using or permitting the use of any unauthorized device in connection with RBU computers 4. maintaining exclusive control over and use of their password, and protecting it from inadvertent disclosure to others 5. ensuring that data under their control and/or direction is properly safeguarded according to its level of sensitivity 6. reporting to the CNC office any incident that appears to compromise the security of RBU information resources. These include missing data, virus infestations and unexplained transactions 7. obtaining CNC office authorization for any uploading or downloading of information to, or from RBU information system if this activity is outside the scope of academic / research activities
6		**Access to Internet**
	a.	Access to Internet is enabled through campus wide fibre backbone network.
	b..	Users are provided with facilities and equipment to access the internet for legitimate work related activity. Sites that are available at all times, this is all sites except c & d below.
	c.	These are categories of sites that are very unlikely to have a legitimate work usage and include: 1. Auction sites 2. Dating sites 3. Gambling sites 4. Game sites
	d.	Sites that contain pornographic and/or objectionable material will be completely blocked as far as is practicable
	e.	The Vice Chancellor will determine the sites to be blocked upon a recommendation from the in charge of CNC.

	f.	CNC will be responsible for managing the internet restrictions and Departments are required to ensure that their internet access is filtered according to this Policy and that all internet management software is installed as determined by CNC.
	g.	Any user who has a legitimate need to access sites under categories c & d may apply to their Head of the Department to gain access.
	h.	Users are prohibited from: creating, viewing, accessing, attempting to access, storing, or displaying inappropriate material either electronically or in hard copy.
	i.	Use of the internet by users is encouraged where such use is consistent with their work or studies or with the goals and objectives of RBU and RBU reserves the right to monitor its Internet on any computer system including PCs.
	j	All users should ensure that the IT Resources provided by the RBU for accessing Internet Services are **not** used for: 1) deliberate unauthorized: a) provision of confidential material concerning the activities of RBU to a third party; b) access to RBU services and facilities by third parties and c) publishing to others, information made available on a one-to-one basis, without the prior express consent of the author. 2) accessing or publishing materials that are or could be considered to be: a) offensive, obscene or containing indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material b) abusive or threatening to others, or serving to harass or bully others c) either discriminatory or encouraging discrimination on racial or ethnic grounds, or on grounds of gender, age, sexual orientation, marital status, disability, political or religious beliefs d) infringing the copyright of another person or business, including intellectual property rights e) designed or likely to cause offence or needless anxiety and f) bringing the RBU into disrepute.

		If such material is accessed accidentally, advice and guidance should be sought, in the case of members of staff, from their Head of the Department, and in the case of students, from their Class Adviser. publishing materials that are or could be considered to be: defamatory; false claims of a deceptive nature; and flaming i.e. using impolite terms or language, including offensive or condescending terms.
	k.	RBU reserves the right to monitor and filter network traffic in order to meet its regulatory obligations.
	k.	Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security
	l.	Users should comply with applicable National /State /Cyber laws and rules and policies of RBU. Examples of rules and policies include, the laws of privacy, copyright, trademark, obscenity and pornography. The IT act 2023 (as amended from time to time) which prohibit hacking, cracking, spoofing and similar activities.
	m.	In-charge of CNC may block content which, in the opinion of the RBU concerned, is inappropriate or may adversely affect the productivity of the users.
	n.	According to the RBU policy, the tethering / hotspotting of internet connection is liable for deactivating the connection
	o.	Accounts and passwords should not under any circumstances be used by any other persons other those to whom they have been assigned by RBU.
	p.	In case, unauthorized use of account is detected or suspected, the account owner should change the password and report the incident to CNC.
	q.	Users shall not use University network and connectivity to get unauthorized access to remote computers which may damage the operations of RBU Network

7.		**Usage of Computer and Networking Equipment**
	a.	Users are expected to take proper care of equipment, and should report any malfunction to the office of CNC. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems. Any Damage/theft must be reported immediately to the Vice Chancellor/ Incharge CNC
	b.	Carrying personal access points, routers or any other networking device and connecting to the network is strictly prohibited. In case if it is required for demonstration to students or labs than prior approval from In charge CNC must be taken.
	c.	Laying of new LAN cable, removing old cables, any modifications in the network infrastructure must be carried out after approval from Incharge CNC
	d.	Faculty and staff are not allowed to carry any IT property of University like printers, projectors etc... (Other than assigned and issued laptops) outside the University, unless and until it is for the University purpose that too by obtaining prior permission of the authorities.
	e.	Department must check the availability of computing hardware available with the central store before going for department level purchase for academic/specific event.
	f.	Usage of telephony facility will be strictly for the University related work only.
8.		**Access to Wireless Networks**
	a.	University WiFi is available in the whole campus and hostels.
	b.	The access to University Wifi is restricted to the registered device only. Usage of University Wifi in an unregistered device by spoofing/tethering will be treated as violation of this policy.
	c.	Even if the access id is different, the registered Wifi user is the sole responsible person for all the communications originated from the registered device.

9.		**Email Policy**
	a.	This Electronic Mail policy applies to all authorized users who are issued a formal (rknec.edu/rbunagpur.in) email account. The purpose of this policy is to establish the University's policy and procedures regarding the use of email facilities. Authorized users of University email facilities are responsible for using and maintaining their email account in accordance with the procedures and guidelines set forth in this Policy.
	b.	Electronic mail, like postal mail, is an official means for communicating University's business. All students, faculty, and staff are expected to read, and shall be presumed to have received and read, all email messages sent to their official email account. Employees of the University including Administration, Faculty and staff must use only rknec.edu/rbunagpur.in email for official email correspondence in the performance of their duties.
	c.	Email for rknec.edu/rbunagpur.in is handled by Google under their Google Apps for Education/G Suite product. As such, Google's Terms of Service also apply. Policies and regulations that apply to other forms of communications and the use of Technology Resources also apply to email facilities.
	d.	Acceptable Use: 1. rknec.edu/rbunagpur.in email is an University's resource intended to be used for University- related business: instruction, instructional support, advising, research, service, administration, and University-related correspondence in support of the University's mission 2. Access to email is an essential tool that imposes on users certain accompanying responsibilities. The same standards of conduct that are expected of students and employees regarding the use of other University facilities, services, and resources apply to the use of email 3. Official email to registered existing students should be sent only to University student email addresses. Emails sent to new students (prior to receiving their rknec.edu/rbunagpur.in account) or non-active students may be sent to their personal email

	e.	Personal Use: University email may be used for incidental personal purposes provided that such use does not: 1. directly or indirectly interfere with the University operation of computing facilities or email service 2. interfere with the email user's employment or other obligations to the University 3. violate this Policy, the University's Acceptable Use policy or any other applicable policy or law, including but not limited to use for personal gain, conflict of interest, harassment, defamation, copyright violation or illegal activities 4. entitle individuals for expectation of privacy with regard to email messages of a personal nature sent or received from University email accounts 5. absolve a user from the responsibilities associated with official communications sent to their University email address in case the user have chosen to have their University email redirected to another email. The University will not be responsible for handling of email by outside vendors.
	f.	Unacceptable Use: In addition, the following specific actions and uses of (rknec.edu/rbunagpur.in) email facilities will be treated as improper: 1. Any use of email that interferes with University activities and functions or does not respect the image and reputation of the University 2. Concealment or misrepresentation of names or affiliations in email messages 3. Alteration of source or destination address of email 4. Use of email for commercial or private business purposes that have not been approved by the administration 5. Use of email to send mass or chain messages in violation of the University's Mass Email Policy 6. Use of email for organized political activity or political solicitation 7. Use of email in violation of the University's Acceptable Use Policy 8. Use of email to harass or threaten other individuals in violation of the University's Non-Discrimination and Non-Harassment Policy or Policy Prohibiting Sexual Misconduct, Relationship Violence, and Stalking 9. Sending unsolicited email messages, junk mail, spam, or advertising material to individuals who did not specifically request such material

		10. Forging or the unauthorized use of email header information 11. Discriminating on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, disability or other classifications protected by law 12. Sending, viewing, or downloading offensive content of any kind, including pornographic material or messages of a sexist, obscene, harassing, threatening, or racist nature 13. Sending, viewing, or downloading messages of a religious or political nature for the purpose of proselytizing and/or soliciting funds or donations 14. Creating or forwarding chain letters, Ponzi, or other pyramid schemes or any type 15. Gambling or any other activities that are illegal, violate any other University policy, or are contrary to the University's interest.
	g.	Authorized Users are responsible for the content of their email messages and should understand that others can use the content as evidence against them. Authorized Users of the University's email facilities whose actions violate this policy or any other University policy or regulation may be subject to revocation or limitation of email privileges as well as other disciplinary actions or may be referred to appropriate external authorities.
	h.	The University respects the privacy of its email users. It does not routinely inspect, monitor, or disclose email. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may deny access to its email services and may inspect, monitor, or disclose email in accordance with the University's Acceptable Use Policy.
	i.	All data files and e-mail communications created and/or maintained on the University's email system are neither private nor confidential. Students, employees and other Users have no right or expectation of privacy in any data files, e-mail communications.
	j.	Vice chancellor of RBU or the authorized representative of the Vice chancellor, has the unrestricted right to access, monitor, retrieve and/or duplicate all data files written or stored on the University's email at any time and for any reason, including all e-mail communications sent or received and any websites visited by a student, employee or other User.

	k.	All data files and e-mail communications created and/or maintained on University's email are an University record and shall be the property of the University. In addition, as an University's record, any data files or e-mail communications are subject to disclosure to law enforcement or government officials or to other third parties through requests under the legal process.
	l.	If there is a reason to believe that an University email account has been used in violation of policies and/or of the law, contents of the email may be inspected and/or disclosed without the prior consent of the employee, student or other User.
	m.	Email, whether or not created or stored on University resources, may constitute an University record subject to disclosure or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of laws concerning disclosure and privacy, or other applicable law. Destruction of such records is governed by the University's Policy.
10		**Bulk Email/SMS policy**
	a.	Specific campus-wide distribution lists will be created, populated and maintained automatically based solely on fields/attributes in the Management Information System (MIS). Requests for new, automated lists must be approved by the Vice Chancellor/ authorized representative of Vice Chancellor.
	b.	Emails to distribution lists are not permitted by addresses outside the University. All email distribution lists will only accept email from a "@rbunagpur.in/rknec.edu" email address. All students, faculty, nonteaching email distribution lists are further restricted and may only be utilized by: • Vice Chancellor • Deans • Specific individuals as delegated by Vice Chancellor

	c.	All e-mails/sms targeted to one or all of the groups noted above must be sent from an official e-mail/sms account. E-mail/sms should not be sent to the official distribution lists from personal e-mail account.
	d.	Faculties are restricted to use mass email/sms communication within their department only. Sending mass emails/sms outside of the department is permitted only with the prior approval of Vice Chancellor.
	e.	In order to maintain the utility of University's mass e-mail/sms system and to reinforce network security best practices, the following criteria have been established for mass e-mail/sms distribution: 1. Messages must directly relate to carrying out the business of the University 2. Messages must share information related to time sensitive issues that affect a significant number of campus community members, and/or 3. Messages must inform a pre-defined target group of an announcement or event related to their specific role within the University, or Messages must relate to significant campus disruptions or occurrences.
	f.	Announcements that do not meet the above criteria of urgency and/or deliver critical University information will not be distributed via mass e-mail/sms. Additionally, inappropriate uses of mass e-mail/sms include: 1. Messages that are not aligned with the mission of the University 2. Messages that are personal in nature 3. Messages that are commercial in nature, with the exception of those messages that are in support of University business and 4. Messages that solicit participation in, support of, or advocacy for events, activities, or campaigns that are not aligned with and/or sanctioned by University.
11.		**Email Account Management**
	a.	All students and employees are assigned an email address (username@rknec.edu/rbunagpur.in), which is the official address to which the University sends email communications, as well as the address that is listed in the email directory and other appropriate University publications.

	b.	Email accounts for students are created automatically the day after a student has confirmed admission at the University
	c.	Email accounts for employees are created automatically the day after Registrar enters their information in the University's employee database, or seven (7) days prior to their official start date, whichever is later.
	d.	The email address is based on the person's legal name as reflected in the Management Information System (MIS). The format is last name followed by initials of first name and middle name. If there is no middle name, the only initial of the first name.
	e.	Student email accounts will remain in effect as long as the student remains enrolled in the University. Students who graduate will have their email accounts deleted after one year of their passing out from the University. Student email account will be deleted immediately upon the account holder being suspended and/or dismissed and/or leaving the University prior to graduating.
	f.	Employees who resign or otherwise terminated from the employment will have their email accounts suspended on their last day of employment. Such employees should be aware that their email accounts may be accessed by their supervisors in order to continue to conduct University operations after they leave. Supervisors seeking such access should send a written request to the Vice Chancellor to obtain access to the account. Once approved, the supervisor will then have 30 calendar days to either forward or copy the work-related email out of the account. After 30 days the account will be deleted.
	g.	Employees who retire from the University and wishes to use email ID assigned by the University should request Vice Chancellor for the continuation of the same. Once approved by Vice Chancellor email Id will be active for next one year only. To continue it further re- approval after every year is needed.
12		**Social media Policy**
		This policy aims to apply a code of conduct for all social media usage by the employees and students of RBU. It envisions users who would strictly abide by the following code of conduct- 1. Do not post or upload views which maybe defamatory, indecent, abusive or derogatory to the name of the University, its employees or the management.

		2. Do not upload or post information that would lead to intellectual copyright violations. 3. Be personally responsible for the content posted on social media sites. The University does not bear any responsibility for the same. 4. Do not use the name RBU on any social media site without prior permission. 5. Do not post any views on behalf of University unless authorized to do so 6. Do not write about, comment on or answer questions regarding any legal matter regarding RBU. 7. Use of social media sites during office hours should complement the work assigned and not interfere with official duties. 8. Do not express anything on social media platforms which may damage the reputation of RBU or its employees. 9. Do not forward or publish any official information, circulars or documents outside the University and to the unregistered persons without prior permission. 10. Do not post or upload any link to chain mail or junk mail on social media platforms. 11. If any departmental social media groups are floated by the departments for the purpose of information exchange, then the head must ensure that only current faculty remains in that group. Anybody who has left the University must be removed immediately.
13.		**Preventing the spread of malicious software**
	a.	Each approved user is required to take positive action to guard against the spread of malicious software e.g. computer viruses, worms or spyware.
	b.	In particular, approved users: 1. must ensure that an effective anti-virus system is operating on any computer which they use to access the IT Resources 2. must not transmit, by email or any other means, any files which are infected with a virus or other malicious software 3. must not open email file attachments received from unsolicited or untrusted sources. 4. must be vigilant when accessing unknown websites as malicious software can be downloaded without their knowledge or consent

14		**Personal use**
	a.	Users must not post or upload personal information on to the RBU website without the consent of authority or without following correct procedures for Web authoring and editing.
	b.	Users must not participate in any online activities that are likely to bring RBU into disrepute, create or transmit material that might be defamatory or incur liability on the part of RBU, or adversely impact on the reputation and image of RBU.
	c.	User must not visit, view or download any material which contains illegal or inappropriate material.
	d.	Users must not knowingly introduce any form of computer virus into the RBU computer network or seek to gain or hack into restricted areas.
	e.	Personal use of the Internet must not cause an increase in service required, eg. storage, capacity and speed or reduce system performance.
	f.	Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such license.
	g.	Users must not use the Internet for financial gain.
	h.	Users must not use the Internet for illegal or criminal activities, such as but not limited to, software and music piracy.
	i.	Users must not use the Internet to send offensive or harassing material to other user.
	j.	Use of the Internet for personal reasons must be limited, reasonable and not distract from work or studies.
	k.	Use of Social Networking sites such, but not limited to, Facebook, LinkedIn , YouTube etc., is allowable to so long as it is reasonable, proportionate and does not interfere with work or studies.

	l.	personal use must not be connected to any purpose or application that conflicts with the RBU's rules, regulations, policies and procedures including this policy.
	m.	In relation to the personal use of IT Resources for Internet Services, if approved users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance, in the case of members of staff, of their Head of the Department, and in the case of students, of their Class Adviser.
15		**Privacy Protection**
	a.	Regardless of the level of protection provided for Internet communications, confidentiality cannot be assured. Confidentiality might be compromised, for example, by law or policy, including this Policy, by unintended redistribution, or by the inadequacy of current technologies to protect against access. Therefore, users should exercise extreme caution in using Internet communications to transmit confidential or sensitive matters
	b.	Users should also be aware that the RBU keeps a log of all accesses to the Internet – including the identifier of the computer accessing the internet, the identification of the site being accessed and the amount of data transferred. These logs are kept by CNC for 15 days. The logs are kept to analyze statistically the RBU Internet traffic.
	c.	The RBU shall only permit the disclosure of sites accessed by an individual without their consent when required by and consistent with law, when there is substantiated reason to believe that violations of law or of RBU policies have taken place.
16.		**Prohibited Downloads**
	a.	Any third party personal antivirus or firewall: Since adequate security has already been provided on all machines via predefined firewall rules, third party firewalls may interfere with these rules thus endangering the network.
	b.	Any proxy servers, private firewall, tunneling software, connectivity sharing software
	c.	Hacking tools of any sort: the use of any such tools on University network is strictly prohibited.

	d.	Games & Movie trailers or previews
	e.	Any other copyrighted content/materials/software which are not appropriate to the user
	f.	The creation and exchange of files/messages that are illegal, offensive, harassing, defamatory, obscene or threatening or that are in conflict with the RBU code of Conduct in the Use of Computer Facilities or national legislation.
	g.	The unauthorized exchange of proprietary information, trade secrets or any other privileged, confidential or sensitive information.
	h.	The creation and exchange of advertisements, solicitations and viruses. The creation and exchange of information in violation of any copyright laws.
17.		**Security**
	a.	If sensitive information is lost, disclosed to parties, or suspected of being lost the CNC or the Vice Chancellor must be notified immediately.
	b.	If any use of malicious information systems has taken place, or is suspected of taking place, the CNC must be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed the CNC must be notified immediately.
	c.	If it may indicate a computer virus infection or similar security problem, all unusual systems, such as missing files, frequent system crashes, misrouted messages and the like must also be reported immediately to the CNC. The specifics of security problems should not be discussed widely, but should be shared on a need-to-know basis.
18.		**Password Management**
	a.	Use a minimum of eight characters for a password.
	b.	Use at least one alphabetic and at least one non-alphabetic character in their password.
	c.	Have facilities to control the number of failed accesses.

	d.	Have time limits for their use.
	e.	Have a secure process for the transmission of new or replacement passwords
	f.	Users must not: • Share the password with anyone. • Write the password down in an insecure location.
	g.	A breach of this policy will incur disciplinary action by the RBU
19.		**Peer-to-Peer Management**
	a.	Use of P2P applications for file sharing and entertainment is deemed to be inappropriate use and will not be permitted.
	b.	P2P usage enable sharing and distribution of copyrighted works, and the Copyright Act makes it illegal to make or distribute copyright materials without proper authorization from the copyright owner.
	c.	RBU will enforce protocol or port level restrictions to prevent P2P activities.
	d.	Any breach of this policy will be managed in accordance with the internet breach policy.
20.		**Enforcement**
	a.	Computing equipment and access to the internet are provided for official purposes and not for personal use. Accordingly, with the prior approval of the Vice Chancellor, the CNC may track the usage, or examine the content, of any computer which has been provided by the RBU, or which is connected to its networks, at any time without prior notice to the staff member using the computer. This includes accessing emails or other electronic communications. Where such access would be appropriate for genuine academic, commercial, or other reasons, an exemption must be obtained from the staff member's Head of the department.

	b.	CNC is responsible for monitoring internet usage and the management of the network in accordance with this policy. This includes: • tracking usage and identifying any concerns • establishing a system for staff to acknowledge the policy when they log on for the first time and for this to be repeated annually.
	c.	CNC will advise the relevant Head of the department of any suspected breaches of this policy. Breaches of this policy may be viewed as serious misconduct which could result in disciplinary action being taken.
	d.	This policy is applicable to all users of RBU. It is mandatory for all users to adhere to the provisions of this policy
	e.	The CNC may suspend, block or restrict the access to an account, when it reasonably appears necessary to do so in order to protect the security, integrity or functionality of the network
	f.	Suspected violations of applicable laws may be referred to appropriate law enforcement agencies
	g.	Alleged violations will be handled through RBU disciplinary procedures applicable to the user
	h.	Penalties include: a simple, verbal warning for the first violation, followed by loss of computer lab privileges for a period of time e.g., two weeks, 12 weeks, or for the remainder of term. Repeated violations can result in dismissal from class or expulsion from the institution. Serious violations may be presented to an institutional Grievance Committee. Violators may also face standard institutional disciplinary action or be required to appear before the Vice Chancellor for appropriate action. If the violation involves illegal activities, civil action may be taken by the institution against the approved user to recover losses.
	i.	Issues of Safety and well-being - Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action.

21.		**Disclaimer**
	a.	RBU reserves the right, without notice, to limit or restrict individual's use and to inspect, copy, remove or otherwise alter any data, file or system which may undermine the authorized use of any computing facility or which is used in violation of RBU rules and policies.
	b.	RBU also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.
	c.	RBU disclaims any responsibility for loss of data or inference with files resulting from its effort to maintain security and privacy.
	d.	RBU reserves the right to amend these policies at any time without prior notice and to take necessary action to comply with applicable laws.
	e.	Due to the insecure nature of electronic communication, the RBU does not accept any liability for damage or loss of whatever nature caused by the use of the Internet Services for personal purposes.
22.		**Advisory Board and Review Mechanism**
	a.	This policy will be reviewed and updated regularly to ensure that it remains appropriate in light of changes to statutory loss and contractual obligations.
	b.	An Advisory Board shall be constituted, comprising of one Professors (who will be coordinator), one Associate Professor, one Assistant Professor and one Non-teaching staff (at least one member in the Board shall be female) as approved by the Apex Committee shall review the implementation of policy at least once in six months, to ensure the compliance of policy and implementation of guidelines stated in the policy. Committee is also empowered to make suggestions for revision of the policy to the Committee responsible for framing this policy.
23.		**Approval Procedure of Policy**
		IT policy of RBU shall be approved by the Governing Council, any revisions that arise subsequently shall be reviewed as said above and forwarded to Governing Council through Member Secretary of the Council for amendments of the policy. On approval of the amendments, revised policy shall be published and circulated to all members appropriately as stated in the Scope (Section 3).

24.		**Policy Revision Process**
		Revision of this policy on suggestions from the Advisory Board or requests from the faculty and staff (at least 20% of total members) may be initiated in consultation with the members of Apex Committee. Committee responsible for framing the earlier version of the policy shall be vested with the responsibility of revising the same. In case, if members are not available, a new Committee shall be formed for revising the policy as approved by the Apex Committee. Revised (Draft) Policy shall be placed before Governing Council for approval and further implementation (with appropriate revision number and effective date).
25.		**References**
	a.	Internet Usage Policy , University of Otago, New Zealand
	b.	Internet Usage Policy , University of Canterbury, New Zealand
	c.	Regulations on the Usage of the Internet from the University, University of Limerick, Ireland
	d.	Information Security Policy, Princeton University, New Jersey
	e.	IT Acceptable Use Policy, University of Auckland, New Zealand
	f.	Email and Internet use policy and Guidelines, University of Greenwich, London
	g.	Internet Acceptable Use Policy, University of Louisville

Avinash J. Agrawal