MANGALORE UNIVERSITY

IT Policy

www.mangaloreuniversity.ac.in

Table of Contents

1. Abbreviation
2. Introduction
3. Scope
4. Objective
5. Roles and Responsibilities
6. Acceptable Use
7. Privacy and Personal Rights
8. Privacy in Email
9. User Compliance
10. Access to the Network
11. Monitoring and Privacy
12. E-mail Access from the University Network
13. Access to Social Media Sites from MU Network
14. Use of IT Devices Issued by MU
15. Security Incident Management Process
16. Intellectual Property
17. Enforcement
18. Deactivation
19. Audit of MU Network Infrastructure
20. Review
21. IT Hardware Installation Policy
22. Software Installation and Licensing Policy
23. Use of IT Devices on MU Network
23.1. Desktop Devices
23.2. Sharing of data
23.3. Use of Portable devices
24. Network (Intranet & Internet) Use Policy
25. Email Account Usage Policy
26. Institutional Repository (IR)
26.1. What is IR (Institutional Repository?
26.2. What Does IR contain?
26.3. Who will be entitled to access Mangalore University IR?
26.4. How will you access the IR?
26.5. Validity Period of Accessibility of IR
26.6. Copyright Violation on IR Use
27. Disposal of ICT equipment
28. Budgetary provisions for ICT
29. Breach of This Policy
30. Revisions to Policy
31. Contact Us

1. Abbreviation

Sl. No.	Abbreviation	Description
1.	MU	Mangalore University
2.	CA	Competent Authority
3.	IA	Implementing Agency
4.	LAN	Local Area Network
5.	GoI	Government of India
6.	IT	Information Technology
7.	ICT	Information and Communication Technology
8.	IP	Internet Protocol
9.	IR	Institutional Repository
10.	EULA	End User License Agreement

2. Introduction

Mangalore University (MU) provides IT resources to support the teaching, research, and administrative activities of the University and to enhance the efficiency and productivity of the stakeholders. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

This document establishes specific requirements for the use of all IT resources at MU. This policy applies to all users of computing resources owned or managed by MU. Individuals covered by the policy include (but are not limited to) MU faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, affiliated colleges and any other entity which fall under the management of Mangalore University accessing network services via MU's computing facilities.

For the purpose of this policy, the term 'IT Resources' includes all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risk and liabilities for the university. It is, therefore, expected that these resources are used primarily for university related purposes and in a lawful and ethical way.

3. Scope

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/ users/ entities, as defined in Section 2, who use the IT resources of Mangalore University.

4. Objective

The objective of this policy is to ensure proper access to and usage of MU's IT resources and prevent their misuse by the users. Use of resources provided by MU implies the user's agreement to be governed by this policy.

- University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.

- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

5. Roles and Responsibilities

The following roles and responsibilities are envisaged from each entity respectively.

1. Mangalore University shall implement appropriate controls to ensure compliance with this policy by their users. Computer Centre shall be the primary Implementing Agency and shall provide necessary support in this regard.
2. Computer Centre shall ensure resolution of all incidents related to the security aspects of this policy by their users. The University shall provide the requisite support in this regard.
3. Use MU's IT resources for those activities that are consistent with the academic, research and public service mission of the University and are not “Prohibited Activities”.
4. All users shall comply to existing national, state and other applicable laws.
5. Abide by existing telecommunications and networking laws and regulations.
6. Follow copyright laws regarding protected commercial software or intellectual property.
7. As a member of the University community / stakeholder, MU provides use of scholarly and/or work-related tools, including access to the Library, certain computer systems, servers, software and databases and the Internet. It is expected from University Community / stakeholders to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of non electronic communication.
8. Users of MU shall not install any network / security device on the network without consultation with the computer centre.
9. It is responsibility of the University Community to know the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
10. As a representative of the MU community, each individual is expected to respect and uphold the University's good name and reputation in any activities related to use of ICT communications within and outside the university.
11. Competent Authority of MU should ensure proper dissemination of this policy.

6. Acceptable Use

* An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.

- A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the University for all use of such resources. As an authorized MU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of MU or a personal computer that is connected to the MU campus wide Network.
- The university is bound by its End User License Agreement (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.
- Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
- No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.
- When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

7. Privacy and Personal Rights

1) *All users of the university's IT resources are expected to respect the privacy and personal* rights of others.
2) Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
3) While the University does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

8. Privacy in Email

While every effort is made to ensure the privacy of MU email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from competent authority, reserves and retains the right to access and inspect stored information with the consent of the user.

9. User Compliance

When an individual uses MU's IT resources, and accepts any University issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of MU and adapt to those changes as necessary from time to time.

10. Access to the Network

10.1. Access to Internet and Intranet

1) A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus wide LAN.
2) MU shall maintain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.
3) 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.

10.2. Access to MU's Wireless Networks (Wi-Fi)

For connecting to a MU's wireless network, user shall ensure the following:

1) A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the MU's wireless network.
2) Wireless client systems and wireless devices shall not be allowed to connect to the MU's wireless access points without due authentication.
3) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

10.3. Filtering and blocking of sites:

1) Computer Centre or any other Implementing Agency (IA) may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
2) Computer Centre or any other Implementing Agency (IA) may also block content which, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.

11. Monitoring and Privacy

1) Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

2) IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.

3) IA may monitor user's online activities on University network, subject to such Standard Operating Procedures of GoI norms.

12. E-mail Access from the University Network

1) E-mail service authorized by MU and implemented by the Computer Centre shall only be used for all official correspondence.
2) More details in this regard are provided in the guidelines of "E-mail Usage of MU".

13. Access to Social Media Sites from MU Network

1) Use of social networking sites by MU users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".
2) User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.
3) User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
4) User shall report any suspicious incident as soon as possible to the competent authority.
5) User shall always use high security settings on social networking sites.
6) User shall not post any material that is offensive, threatening, obscene, infringes Copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
7) User shall not disclose or use any confidential information obtained in their capacity as an employee of the university.
8) User shall not make any comment or post any material that might otherwise cause damage to the University's reputation.

14.Use of IT Devices Issued by MU

IT devices issued by MU to a user shall be primarily used for academic, research and any other university related purposes and in a lawful and ethical way and shall be governed by the practices defined in the Section “Use of IT Devices on MU Network”. The aforesaid section covers best practices related to use of Lap tops, desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

15.Security Incident Management Process

1) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of University’s data.
2) IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the university.
3) Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.
4) Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.
5) IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

16.Intellectual Property

Material accessible through the MU’s network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use MU’s network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

17.Enforcement

1) This policy is applicable to all the users of MU as specified in Section 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.
2) Each entity of MU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.

18.Deactivation

1) In case of any threat to security of MU's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.
2) Subsequent to such deactivation, the concerned user and the competent authority of the university shall be informed.

19.Audit of MU Network Infrastructure

The security audit of MU network infrastructure shall be conducted periodically by an organization approved by the University.

20.Review

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee (ICT) with the approval of the Competent Authority of the University.

21.IT Hardware Installation Policy

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the Chairman of the department should make an arrangement and make a person responsible for compliance. If it is a multiple user device at computer centre/ cyber centre of the University, the Director, Computer centre shall make a person responsible for compliance.

B. What are End User Computer Systems

Apart from the client PCs used by the users, the university will consider servers not directly administered by Computer Centre, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the Computer Centre, are still considered under this policy as "end- users" computers.

C. Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

E. Network Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the office / centre, University Computer Maintenance Company / staff attached with Computer Centre will attend to the complaints related to any maintenance related problems.

22.Software Installation and Licensing Policy

Any computer purchases made by the individual departments/ projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so. University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

B. Use of software on Desktop systems

a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.
b. Any software installed should be for activities of the university only.

C. Antivirus Software and its updating

Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

D. Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

23.Use of IT Devices on MU Network

This section provides the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on MU's network.

23.1. Desktop Devices

1) Use and Ownership

Desktops shall normally be used only for transacting university's works. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

2) Security and Proprietary Information

a. User shall take prior approval from the Computer Centre / IA to connect any access device to the MU's network.
b. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy of the application.
c. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.
d. Users shall ensure that updated virus-scanning software is running in all systems.
   Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

e. User shall report any loss of data or accessories to the CC/ IA and competent authority of MU.
f. User shall obtain authorization from the competent authority before taking any MU issued desktop outside the premises of the university.
g. Users shall properly shut down the systems before leaving the office/ department.
h. Users shall abide by instructions or procedures as directed by the Computer Centre from time to time.
i. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA (Computer Centre) for corrective action.

23.2. Sharing of data

Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

23.3. Use of Portable devices

Devices covered under this section include MU issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices shall be governed by the following:

a. User shall be held responsible for any unauthorized usage of their MU issued access device by a third party.

b. Users shall keep the MU issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. classrooms, meeting rooms, restaurants etc.).

c. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.

d. Computer Centre shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, f possible.

e. Users shall wipe or securely delete data from the device before returning/ disposing it off.

f. Lost, stolen, or misplaced devices shall be immediately reported to the IA/ and the competent authority.

g. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

24.Network (Intranet & Internet) Use Policy

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Computer Centre is responsible for

the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to Computer Centre.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the Computer Centre. Following a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN (VLAN) created against each entity or objective. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location. As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.
An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

B. DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the services run by the Computer Centre.

Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration. Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. Running Network Services on the Servers

a. Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Centre in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

b. Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

c. Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

d. Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.

e. Network traffic will be monitored for security and for performance reasons at Computer Centre.

g. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

D. Internet Bandwidth obtained by Other Departments

a. Internet bandwidth acquired by any department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource.

b. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.

c. IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to Computer Centre.

d. Non-compliance to this policy will be direct violation of the university's IT security policy.

25.Email Account Usage Policy

MU provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email with Mangalore University's domain. In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for normal University communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to http://gmail.com with their User ID and password. For obtaining the university's email account, user may contact Computer Centre for email account and default password by submitting an application in a prescribed proforma. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

2) Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3) While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4) User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5) User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious in nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.

6) User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

7) User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

8) While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

9) Impersonating email account of others will be taken as a serious offence under the IT security policy.

10) It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

11) All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible. The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other service providers such as Gmail, Hotmail, Yahoo, RediffMail etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

26.Institutional Repository (IR)

Mangalore University shall be providing services related to Institutional Repository (IR) through Central Library of the university as per the following policies

26.1. What is IR (Institutional Repository)?

A University-based institutional repository (IR) is a set of services that a University Library offers to the members of its community for the management and dissemination of digital materials created by the University or institution and its community members. It is most essentially an organizational commitment to the stewardship of these digital materials including long-term preservation, access and dissemination of e-resources of an organization to its users.

26.2. What Does IR contain?

IR of the institution contains a wide variety of documents depending on the policy of the institution. Most common are the outputs of research journal articles (pre-print and postprint), conference papers, technical reports, computer programs, preservations, technical manuals, Video and audio recordings, e-Books, Seminar and Webinar lectures, Theses and Dissertations and Rare books etc. Grey literature is as important as published outputs in the IR. Institutional Repository (IR) also contains other items such as convocation addresses, student handbooks, as well as teaching materials quotes sources which suggest that a repository should be integrated with the University's course management system and display e-learning features. In practice, however, Mangalore University institution repository (IR) will provide a basic repository of such resources available through online which focus on research and academic publications.

26.3. Who will be entitled to access Mangalore University IR?

Mainly the bonafide members i.e. faculty members, research scholars, students and other staff members having institutional e-mail IDs (i.e. @MU.ac.in) are authorized members to access the IR of Mangalore University.

26.4. How will you access the IR?

The registered members through their institutional e-mail address can log-in to IR link http://MUir.inflibnet.ac.in and browse the MU IR and can download digital materials in pdf format purely for their academic purpose subject to provision of giving general information of the member provided in the Mangalore University IR portal.

26.5. Validity Period of Accessibility of IR

Teachers, researchers and students are authorized to access MU IR as long as they are in the University. The moment the tenure in the University or the course is completed and the no dues certificates are issued from the University Library authority, the validity of access to MU IR will be withdrawn.

26.6. Copyright Violation on IR Use

Mangalore University IR digital materials are mainly grey literature. Any downloaded digital materials from the IR comes under the purview of copyright. The downloaded permissible materials cannot be reprinted and sold in the market for commercial purpose further. If any member found violating such copyright act shall be treated as per the provisions of copyright act-

1957. The created user-id and password are person specific and cannot be transferred to any other person and subject to the violation of SOPs of Mangalore University IR.

27.Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the university.

28.Budgetary provisions for ICT

At Mangalore University, use of ICT facilities have been encouraged as it is located in remote area of the country. This has always been a leverage to march shoulder to shoulder with rest of the universities. In view of these scenarios, MU intends to provide budgetary provisions as follows:

1) Budgetary provisions should be made under recurring grants (OPEX) to maintain all the existing ICT infrastructure for smooth functioning of all the ICT enabled services.
2) Adequate budgetary provisions under capital head (CAPEX) should be kept for upgradation and augmentation of ICT infrastructure
3) Budgetary provisions under capital grants should also be allocated for implementation of newer ICT solutions from time to time.
4) In MU, there has been an increase of 10% enrolment of students every year. Keeping in view of this increase and for the benefit of the students, a budget of 10% of the total budget of the university should be earmarked for ICT facility particularly for students.

29.Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk admin@MU.ac.in. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.
If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

30.Revisions to Policy

The University reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the MU

website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

31.Contact Us

If you have any queries in relation to this policy, please contact:

Director, Computer Centre
Mangalore University
Phone: 0824-2287515
Email: computercentre@mangaloreuniversity.ac.in