IT POLICY & GUIDELINES

February 2020, Version 1.0

Modern College of Arts, Science and Commerce (Autonomous),

Shivajinagar, Pune

Table of Contents

1. Abbreviation

Sr. No.	Abbreviation	Description
1	MCASC	Modern College of Arts, Science and Commerce (Autonomous)
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	DHCP	Dynamic Host Configuration Protocol

10	**IR**	**Institutional Repository**
11	**EULA**	**End User License Agreement**
12	**CAPEX**	**Capital Expenditure**
13	**OPEX**	**Operational Expenditure**

2. Introduction

Modern College of Arts, Science and Commerce (Autonomous) provides IT resources to support the educational, instructional, research, and administrative activities of the MCASC and to enhance the efficiency and productivity of the employees and students. 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 MCASC. This policy applies to all users of computing resources owned or managed by MCASC. Individuals covered by the policy include (but are not limited to) MCASC 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 MCASC accessing network services via MCASC's computing facilities.

3. PURPOSE

This policy defines the IT rules that are required to be implemented in order to ensure the confidentiality, integrity and availability of information and information systems at MCASC.

For the purpose of this policy, the term 'IT Resources' includes all MCASC owned, licensed, or managed hardware and software, and use of the MCASC 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 MCASC. It is, therefore, expected that these resources are used primarily for MCASC related purposes and in a lawful and ethical way. The IT Policy is a live document and the same will be reviewed once a year. The IT Policy is support by the Process Handbook which details the process further; both the documents must be read and understood together.

3. Scope

Policies from this document apply to information and information systems across MCASC. This policy governs the usage of IT Resources from an end user's perspective. All users such as permanent employees, temporary employees, trainees, teachers, students, Parents and other related third party personnel (all individuals/ users/ entities, as defined in Section 2 who use the IT Resources of MCASC) of MCASC shall adhere to this policy.

4. Objective

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

1. MCASC IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the MCASC on the campus.

2. This policy establishes MCASC -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 MCASC.

3. 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) MCASC 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. Implementing Agency shall provide the requisite support in this regard.

3) Use MCASC's IT resources for those activities that are consistent with the academic, research and public service mission of the MCASC and are not "Prohibited Activities".

4) All users shall comply with 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 MCASC community, MCASC 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 MCASC Community 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 nonelectronic communication.

8) Users of MCASC shall not install any network/security device on the network without consultation with the IA.

9) It is responsibility of the MCASC Community to know the regulations and policies of the MCASC that apply to appropriate use of the MCASC's technologies and resources. MCASC Community is responsible for exercising good judgment in the use of the MCASC'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 MCASC community, each individual is expected to respect and uphold the MCASC's good name and reputation in any activities related to use of ICT communications within and outside the university.

11) Competent Authority of MCASC 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 MCASC for all use of such resources. As an authorized MCASC user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of MCASC or a personal computer that is connected to the MCASC campus wide Local Area Network (LAN).

· The MCASC 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

· **All users of the MCASC's IT resources are expected to respect the privacy and personal rights of others.**

· **Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).**

· **While the MCASC 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 MCASC email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct MCASC business, there may be instances when the MCASC, 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 MCASC's IT resources, and accepts any MCASC 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 MCASC and adapt to those changes as necessary from time to time.

10. Access to the Network

10.1. Access to Internet and Intranet

· **A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the MCASC Campus wide LAN.**

· **2) MCASC 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 the 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 MCASC's Wireless Networks

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

- **A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the MCASC's wireless network.**

- **2) Wireless client systems and wireless devices shall not be allowed to connect to the MCASC'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:

- **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 MCASC, is inappropriate or may adversely affect the productivity of the users.**

11. Monitoring and Privacy

- **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 MCASC provided devices under intimation to the user. This includes items such as files, photos, e-mails, posts on any electronic media, Internet history etc.**

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

12. E-mail Access from the MCASC Network

· **E-mail service authorized by MCASC and implemented by the Computer Centre shall only be used for all official correspondence.**

· **More details in this regard are provided in the "E-mail Usage Policy of MCASC".**

13.Access to Social Media Sites from MCASC Network

· **Use of social networking sites by MCASC users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".**

· **User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.**

· **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.**

· **User shall report any suspicious incident as soon as possible to the competent authority.**

· **User shall always use high security settings on social networking sites.**

· **User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.**

· **User shall not disclose or use any confidential information obtained in their capacity as an employee of the MCASC.**

· **User shall not make any comment or post any material that might otherwise cause damage to MCASC's reputation.**

14. Use of IT Devices Issued by MCASC

IT devices issued by the MCASC to a user shall be primarily used for academic, research and any other MCASC 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 MCASC Network". The aforesaid section covers best practices related to use of 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 MCASC'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 MCASC'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 MCASC'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 MCASC 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 MCASC 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 MCASC'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 MCASC shall be informed.

19. Audit of MCASC Network Infrastructure

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

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 MCASC.

21. IT Hardware Installation Policy

MCASC 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 department Head should make an arrangement and 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 earthling 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 MCASC

For all the computers that were purchased by the MCASC centrally and distributed by the Estate Branch, MCASC Computer Maintenance Cell 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, MCASC IT policy does not allow any pirated/unauthorized software installation on the MCASC owned computers and the computers connected to the MCASC campus network. In case of any such instances, MCASC 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.

MCASC 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 MCASC only.

C. Antivirus Software and its updating

Computer systems used in the MCASC 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

The objectives of the Backup policy are to ensure:

- **Maintenance of the integrity and availability of information within MCASC**
- **Definition of routine procedures for carrying out data backup and restoration.**
- **Restoration of data essential to the business within the defined timelines.**

SCOPE

This policy applies to all users of MCASC. This policy targets:

i. IT Applications (FAS, ESMS, EPMS, ETAT-1, Argus, Tableau)

ii. IT Applications in Cloud (Buddy, Webgenie, Email)

iii. End Point devices

STATEMENTS

- **All applications data(including databases), system configuration files shall be backed up in accordance with the processes & procedures laid down in the process handbook**

- **All End Point data must be backed up the individual user on the shared folder provided by IT or Official Google Drive, IT will centrally backup the shared folder.**

- **In Schools and Regional Locations, backup of critical systems must be maintained on the external drive by departments**

- **Backups must be tested periodically by carrying out restoration to check integrity of the backed up data and also the ability to restore data whenever required.**

- **Backup media must be clearly identified, labeled, logged and stored securely. Access to backup media must be restricted on a 'need to know' basis.**

- **Backups shall be stored for a period which is as per legal, regulatory and business requirements.**

- **Back-up shall be stored securely at the on-site location. If possible, data should also be stored securely at an off-site location.**

- **Relevant backup records shall be maintained to track successful/unsuccessful backup attempts**

23. Use of IT Devices on MCASC 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 MCASC's network.

23.1. Desktop Devices

1) Use and Ownership

Desktops shall normally be used only for transacting MCASC'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 IA to connect any access device to the MCASC'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 IA and competent authority of MCASC.

f. User shall obtain authorization from the competent authority before taking any MCASC issued desktop outside the premises of the MCASC.

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 MCASC 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 MCASC issued access device by a third party.

b. Users shall keep the MCASC 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, if 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 MCASC, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the MCASC IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the MCASC's network should be reported to Computer Centre.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the MCASC 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 MCASC 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 MCASC 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 MCASC'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 MCASC Network connects. MCASC 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.

f. 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 MCASC under any research programme/project should ideally be pooled with the MCASC's Internet bandwidth, and be treated as MCASC's common resource.

b. Under particular circumstances, which prevent any such pooling with the MCASC Internet bandwidth, such network should be totally separated from the MCASC'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 MCASC gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the MCASC 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 MCASC's IT security policy.

25. Email Account Usage Policy

MCASC 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 MCASC's domain. In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the MCASC's administrators, it is recommended to utilize the MCASC's e-mail services, for formal MCASC 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 MCASC communications are official notices from the MCASC to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, and general MCASC 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 MCASC's email account, user may contact Computer Centre for email account and default password by submitting an application in a prescribed proforma.

Password Policy:

The objective of the Password policy is to ensure:

- **Creation of a standard for generating strong passwords, the protection of those passwords, and defining the frequency of change.**

SCOPE

This policy applies to all users of MCASC. This policy targets:

i. Applications within the organization – FAS, EPMS, ESMS, Active Directory (AD) at HO LMS, MS teams, Google, …..

ii. Email : as Enforced by google email

Statements:

- **Password policy is applicable for all users, accounts and Information System**
- **Password policy must be enforced through appropriate configuration of the operating systems, applications, databases, network devices and access management systems.**
- **After maximum of five unsuccessful login attempts, the account must be locked out.**
- **Any account locked out due to invalid login attempts must be reset by the IT Department only on written request / after obtaining adequate authentication about genuineness of the user where system does not support automatic password resets.**
- **Passwords must be at least eight characters in length.**
- **Passwords must be complex, consisting of alphabets, numerals and special characters.**
- **Passwords at minimum must be changed every 90 days. Applications and systems must enforce this change.**
- **Passwords must not be shared. Users shall be accountable for all actions under their account.**

· **Password must never be displayed in clear text or stored in readable form including but not limited to databases, batch files, and automatic login scripts keys or in any other locations.**

· **All users shall be given an initial temporary password. Default passwords shall be communicated securely to end user and must be immediately changed upon first login by the user.**

· **Exceptions to the password policy shall be subject to approvals from the Principal, after understanding and documenting the risks involved of not implementing the policy and nature of compensating controls.**

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 MCASC'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 MCASC'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 MCASC's campus network, or by using the resources provided by the MCASC to the individual for official use even from outside.

26. Institutional Repository (IR)

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

26.1. What is IR (Institutional Repository)?

A MCASC-based institutional repository (IR) is a set of services that a MCASC Library offers to the members of its community for the management and dissemination of digital materials created by the MCASC 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 post print), 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 MCASC's course management system and display e-learning features. In practice, however, MCASC 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 MCASC IR?

Mainly the bonafied members i.e. faculty members, research scholars, students and other staff members having institutional e-mail IDs (i.e. @moderncollegepune.edu.in) are authorised members to access the IR of MCASC.

26.4. How will you access the IR?

The registered members through their institutional e-mail address can log-in to IR link http://moderncollegepune.edu.in and browse the MCASCIR and can download digital aterials in pdf format purely for their academic purpose subject to provision of giving general information of the member provided in the MCASC IR portal.

26.5. Validity Period of Accessibility of IR

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

26.6. Copyright Violation on IR Use

MCASC IR digital materials are mainly grey literature. Any downloaded digital materials from the IR come 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 MCASC 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 MCASC.

28. Budgetary provisions for ICT

At MCASC, 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, MCASC intends to provide budgetary provisions as follows:

1) Budgetary provisions should be made under recurring grants (OPEX) to maintain the entire 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 MCASC, 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 MCASC 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@moderncollegepune.edu.in . On receipt of notice (or where the MCASC otherwise becomes aware) of any suspected breach of this Policy, the MCASC reserves the right to suspend a user's access to MCASC'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 MCASC's disciplinary procedures.

30. Revisions to Policy

The MCASC 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 MCASC website and by continuing to use the MCASC'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:

Joint Director, Computer Centre

Phone:

Email: admin@moderncollegepune.edu.in

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID (For Teachers & Staff only)

First Name :

Middle Name :

Last Name :

Department/ Branch :

Current Email

address* :

Mobile Number :

Note:

1. Please spell the names and all other information sought above correctly.

2. *This Email address should be currently used by you.

3. The filled in form should be submitted after getting duly signed from respective Head of the Department/ Controlling Officer.

4. An official Email address would be created within 48 hrs. - 72 hrs.

5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department/ Controlling Officer)

Appendix – II: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID (For Research Scholars only)

First Name :

Middle Name :

Last Name :

Department :

Name of the PI :

Name of the Project :

Duration of Research :

Current Email

address* :

Phone Number :

Admission Year* :

Note:

1. Please spell the names and all other information sought above correctly.

2. *This Email address should be currently used by you.

3. The filled in form should be submitted after getting duly signed from respective Head of the Department and Principal Investigator.

4. An official Email address would be created within 48 hrs. - 72 hrs.

5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Principal Investigator)

Appendix – III: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS (For Students only)

Name :

Father's Name :

Gender :

DoB :

Department :

Course :

Semester :

Roll No. :

Email address* :

Mobile Number :

Note:

1. Please spell the names and all other information sought above correctly.

2. *This Email address should be currently used by you.

3. The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of the Head of the Department)

Appendix – IV: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS (For Employees only)

Name :

Father's Name :

Gender :

DoB :

Department/ Branch :

Email address* :

Mobile Number :

Note:

1. Please spell the names and all other information sought above correctly.

2. *This Email address should be currently used by you.

3. The filled in form should be submitted after getting duly signed from respective Controlling Officer.

(Signature of the Controlling Officer)