

**Email Policy
of
Management Development Institute,
Gurgaon**

**December 2015
Version 2.0**



DOCUMENT MANAGEMENT INFORMATION

Document Name	Email Policy
Document Number	
Document Owner	
Security Classification	Restricted
Document Status	Draft
Date of Release	

VERSION CONTROL

Version No.	Issue Date	Approval Date	Change Details	Approved by
1.0	29 June 2010	02 July 2010		Director
2.0	02 Dec 2015			

DOCUMENT CONTACT LIST

Role	Name	Contact Number	Email Address
Chairperson (Computer Center)			
Coordinator Computer Center			
Chief System Administrator			

Table of Contents

1. Policy	4
1.1 Introduction	4
1.2 Purpose of the Email Policy	4
1.3 Policy Scope and Applicability.....	4
2. Use of Email Services	5
2.1 Roles specified for implementation of the Policy.....	6
2.2 User's Role	7
2.3 Regular accessing of Emails	7
2.4 MDI property.....	7
2.5 MDI records.....	8
2.7 Representation.....	8
2.8 Interference	8
3. Group Email Policy	8
4. Security and Confidentiality.....	9
3.1 Scrutiny of Emails/Release of logs.....	10
3.2 Security Incident Management Process	10
4. Audit of Email Services.....	11
5. Policy Dissemination	11
6. Review.....	11
7. Definitions.....	11
8. Best practices	12

1. Policy

1.1 Introduction

Electronic mail (Email) is pervasively used and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of Email.

This Email Policy has been developed in response to the acknowledged need for guidelines describing the acceptable use of the MDI's Email and related services and facilities. The Policy is maintained and regulated by the Computer Center under the overall responsibility of Competent Authority.

The Policy will be distributed to users of the Email and related services and facilities. There will also be periodic re-issue of the Policy, supported by sign-up acceptance by users of the facilities. The Policy will be reviewed and, if necessary, amended from time-to-time, with particular regard to the expected developments in the operational use of the Email system, and by reference to the development of recognised best practice.

1.2 Purpose of the Email Policy

The Email Policy provides guidance about acceptable use, for the purpose of sending or receiving Email messages and attachments. The Policy also describes the standards that users are expected to observe when using these facilities for Email, and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

The purpose of this Policy is to ensure that:

- The MDI community is informed about the applicability of policies and laws with regard to Email;
- Email services are used in compliance with those policies and laws;
- Users of Email services are informed about how concepts of privacy and security apply to Email; and
- Disruptions to MDI's Email and other services and activities are minimised.

1.3 Policy Scope and Applicability

This Policy applies to all Email services provided by MDI and to all users of such services; and to all MDI records in the form of Email in the possession of MDI employees.

MDI provides an Email account to every faculty, staff member and student of MDI for the purposes of teaching and learning, research, administration and community service.

The directives contained in this policy must be followed by all of them with no exceptions.

Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

2. Use of Email Services

The purpose of this policy is to ensure secure access and usage of MDI Email services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of MDI's Email service amounts to the user's agreement to be governed by this policy.

The Email address supplied by MDI is considered to be the official Email contact point for MDI faculty, staff and students, and official MDI Email correspondence may be delivered to this address.

Only the e-mail services provided by MDI, shall be used for official communications. The Email services provided by other service providers shall not be used for any official communication.

MDI permits this account to be used for limited incidental personal purposes. However, it is most concerned to ensure that the account is used as effectively as possible in support of the above purposes and to facilitate the work of MDI. An MDI Email account may not be used for engaging in non-MDI business or for personal gain, except if permitted by other MDI policies.

Official Email id provided by MDI can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

Email accounts may also be used for the submission and return of student assignments and other specific uses, but only where the relevant faculty or administrative Unit has specifically authorised this, and where the guidelines and conditions for such submission/return, which have been specified by that Faculty or Unit, have been fully complied with.

The sender of Email will be considered responsible for the content of the message. Consequently the sender will be responsible for any cause of damage, loss of good will, or loss of monetary terms if the message that has caused it originates from “mdi.ac.in” domain or any other official domain, and MDI would not be responsible for it.

Examples of inappropriate use of the e-mail service

- i) Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.
- ii) Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.
- iii) Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other person's user ids or using a false identity.
- iv) Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.
- v) Creation and exchange of information in violation of any laws, including copyright laws.
- vi) Wilful transmission of an e-mail containing a computer virus.
- vii) Misrepresentation of the identity of the sender of an Email.
- viii) Use or attempt to use the accounts of others without their permission.
- ix) Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, sending e-mails with obscene material, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation of the account. The users will have to face consequences as decided by the investigation committee (appointed by the Director, MDI) depending on the nature of violation.

2.1 Roles specified for implementation of the Policy

The following roles are specified for using the MDI e-mail service. The official identified for the task shall be responsible for the management of the entire user base configured under that respective domain.

2.1.1 Competent Authority : Director, Chairperson (Computer Center)

2.2.2 Designated officer : Coordinator Computer Center, Chief System Administrator (CSA)/ Chief Information Officer (CIO)

2.2.3 Computer Center: Senior System Analyst (SSA), System Analyst, System Administrator

Competent Authority of the user organization shall ensure that training and awareness programs on e-mail security are organized at regular intervals. Designated officer/ Computer Center shall provide the required support.

Competent authority shall introduce a process to ensure that e-mail id is either deactivated/deleted/password changed, prior to giving "no dues" to a user.

The Computer Center shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

The Computer Center shall be responsible for maintaining an updated list of Email users.

As far as possible, the format of the Email should include "firstname.lastname" and standardization of Email should be done.

The Computer Center shall provide the e-mail services based on the Service Level Agreement (SLA) with E-mail service provider.

Forgot Password: In order to empower a user to reset his/her password, the Computer Center shall provide the "Forgot password" service. This service allows a user to reset the password without the intervention of Computer Center support.

2.2 User's Role

- a) The User is responsible for any data/e-mail that is transmitted using the MDI e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
- b) Use of Secure Passwords: All users accessing the e-mail services must use strong passwords for security of their e-mail accounts.
- c) The user should change passwords on a periodic basis or as per the password policy. More details about the password policy are available in "Password Policy" of MDI.
- d) Sharing of passwords is prohibited. Users must ensure that information regarding their password or any other personal information is not shared with anyone.
- e) Auto-save of password in the MDI e-mail service shall not be permitted due to security reasons.
- f) The users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.
- g) The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.
- h) Back up of important files/ individual e-mails stored in the folders shall be taken by the user at regular intervals. The Computer Center shall not be responsible for any accidental deletion of e-mails by the user.
-) Computer Center is not responsible for the retention of the Email messages. Users are responsible for taking periodic backup and archival of their respective Emails.

2.3 Regular accessing of Emails

It is important for members of faculty, staff and students to access and read Email messages sent to their MDI Email account on a timely basis, and they will be presumed to do so for the purposes of the types of Emails specified in section 2.1.

2.4 MDI property

MDI Email services are MDI facilities; all MDI Email addresses are owned by MDI; and all Email which is in support of MDI business, whether or not the equipment, software, or facilities used to create or store the Email record are owned by MDI, are MDI records.

MDI reserves the right to install and operate filtering equipment, software or procedures to prevent the entry into MDI of Email traffic that is contrary to law or which is incompatible with the objectives of MDI.

2.5 MDI records

Emails that are sent or received using a non-MDI address but which relate to official MDI business constitute official MDI records. In these cases, normal record keeping requirements must be observed.

2.6 Restrictions on Email use

MDI Email services may not be used for: unlawful activities; commercial purposes not under the auspices of MDI; personal financial gain; or uses that violate other MDI policies or guidelines.

2.7 Representation

Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the MDI or any of its units unless appropriately authorised (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing MDI. An appropriate disclaimer, for example, could be: "These statements are my own, not those of the MDI".

2.8 Interference

MDI Email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of Email or Email systems. Such uses include, but are not limited to, the use of Email services to: (i) send or forward Email chain letters; (ii) "spam", that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited Email; and (iii) "letter-bomb", that is, to resend the same Email repeatedly to one or more recipients to interfere with the recipient's use of Email.

3. Group Email Policy

Group Email is an efficient way to communicate MDI-related information to a group of students, faculty and/or staff. However, when used improperly, the group Email system becomes an ineffective and unwelcome communication tool. This group Email policy has been implemented to improve the effectiveness of Email communications to students, faculty and staff and to ensure group Email communication is professional, clear and relevant. This policy applies to all Email users within the "mdi.ac.in" or any other official mdi domain, including students, faculty and staff.

Users should send Emails on their own behalf, and the content of a group Email sent is the responsibility of the owner of the address in the "From:" address line. Faculty and staff should not send group Emails on a student's behalf, nor should students send Group Emails for faculty and staff.

Relevance: Group Email should be used to communicate with students, faculty, and staff about MDI's educational services and business and administrative matters. Information sent must be related to the group being mailed.

In this context it has been noticed that the group mails are often misused by sending Emails which are not relevant to the entire faculty or all the staff. It is suggested that the group mails should be used only by the activity heads. Any Email targeted for all faculty and/ or all staff but not originating from activity head should be routed through the respective activity head so as to avoid possibility of misuse of the group-address.

Reply to group Email: Do not "Forward" or "Reply to All" with group Emails. If a response is requested, reply directly to the sender only.

4. Security and Confidentiality

MDI attempts to provide secure and reliable Email services. Computer Centre operations and support staff looking after Email services are expected to follow sound professional practices in providing for the security of Email records, data, application and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of Email cannot be guaranteed. Furthermore, operators of Email services have no control over the security of Email that has been downloaded to a user's computer. As a deterrent to potential intruders and to misuse of Email, Email users should employ whatever protections (such as passwords) are available to them.

The confidentiality of Email cannot be assured. Such confidentiality may be compromised by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorised access. Users of MDI Email services, therefore, should exercise extreme caution in using Email to communicate confidential or sensitive information.

Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent by the Computer Center. Updation of personal e-mail id (preferably from a service provider within India), in addition to the mobile number, shall also be mandatory in order to reach the user through an alternate means for sending alerts.

Reset/ Change of Password: An authorized person under the Computer Center can create/delete/change the password of user ids under the MDI domain, if required. Where required such requests need to be forwarded with complete details to the Computer Center Help Desk (cchelp@mdi.ac.in).

User addresses and passwords of Email accounts, which are not used for more than 3 months, shall be suspended.

If any faculty or staff member goes on long-term leave from MDI, their Email accounts will be kept active during the leave duration. However, their Email account will be removed from any group Email address lists.

If any faculty member resigns from the services of MDI, his/her Email address will be immediately removed from any group lists.

Graduating student accounts will be deleted 30 days after their convocation.

It is recommended for faculty users to use VPN for secure authentication as deemed appropriate by the competent authority when using MDI Email facility from outside MDI premises.

3.1 Scrutiny of Emails/Release of logs

Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the Computer Center would be done only as per the IT Act 2000 and other applicable laws.

The Computer Center will maintain logs for a period of one year.

3.2 Security Incident Management Process

A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Government data. Security incidents can be due to factors like malware, phishing, loss of a device, compromise of an e-mail id etc.

Any security incident, noticed or identified by a user must immediately be brought to the notice of the Computer Center.

In case a compromise of an e-mail id is detected by the Computer Center, an SMS alert shall be sent to the user on the registered mobile number. In case an “attempt” to compromise the password of an account is detected, an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromise), the Computer Center reserves the right to reset the password of that particular e-mail id under intimation to the Coordinator, Computer Center.

In case of a situation when a compromise of a user id impacts a large user base or the data security at MDI, the Computer Center shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user and the designated officer subsequently. SMS shall be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.

It shall be within the right of the Computer Center to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

4. Audit of Email Services

The security audit of MDI Email services shall be conducted annually.

5. Policy Dissemination

- a) Competent Authority should ensure dissemination of the Email policy.
- b) Orientation programs for new faculty, staff, students shall include a session on the e-mail policy by the designated officer.

6. Review

Future changes in this Policy, as deemed necessary, shall be made in consultation with stakeholders after due approval of competent authority.

7. Definitions

Email services: Information technologies used to create, send, forward, receive, store, or print Email.

MDI record (in the form of Email): Any Email that is in support of MDI business, whether or not the equipment, software, or facilities used to create, or store the Email record are owned by MDI.

Use of Email services: To create, send, forward, reply, copy, store, print, or possess Email messages. For the purpose of this Policy, receipt of Email is excluded from this definition to the extent that the Email user does not have control over the Email received.

Email address/ Email account: The officially recognised MDI Email address as allocated by Computer Center on enrolling as a student or joining MDI as faculty or staff.

8. Best practices

MDI considers email as an important means of communication and recognizes the importance of proper email content in conveying a professional image. Users should take the same care in drafting an email as they would for any other communication. Therefore MDI wishes users to adhere to the following email guidelines:

- **Writing emails:**
 - Write well-structured emails and use short, descriptive subjects.
 - This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smileys however, is not encouraged.
 - Signatures must include your name, designation and MDI name. A disclaimer will be added underneath your signature (see Disclaimer below)
 - Users must spell check all mails prior to transmission.
 - Do not send unnecessary attachments. Compress attachments larger than 5 MB before sending them.
 - If you need to send files of over 10 MB, do not send these via email; contact your Administrator to find alternate methods for sending the files.
 - Do not write emails in capitals.
 - Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
 - Only mark emails as important if they really are important.
- **Maintenance:**
 - Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

QUESTIONS

If you have any questions or comments about this Email Policy, please contact the Competent Authority.

If you do not have any questions, MDI presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

DECLARATION

I have read, understand and acknowledge receipt of the Email Policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

Signature: _____

Date: _____