FTK-Centre for Information Technology
Jamia Millia Islamia

ICT POLICY DOCUMENT

An internet usage policy provides employees with rules and guidelines about the appropriate use of organization's equipment, network and Internet access. The purpose of this policy is to help protect both the organization and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to or there could be serious repercussions, thus leading to fewer security risks for the organization as a result of employee negligence. The Internet Usage Policy is an important document that must be signed by all employees upon starting work. Below is a Sample Internet Usage Policy that covers the main points of contention dealing with Internet and computer usage.

Internet usage policy

This Internet Usage Policy applies to all employees of Jamia Millia Islamia who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees of Jamia Millia Islamia is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through JMI is a privilege and all employees must adhere to the policies concerning Computer, Email and Internet usage. Violation of these policies could result in disciplinary and/or legal action. Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

Computer, email and internet usage

- JMI employees and students are expected to use the Internet responsibly and productively.
- Internet facility is primarily limited to academic and research purposes.
- Employees may occasionally use the facility for personal communication through personal emails
- All Internet data that is composed, transmitted and/or received by JMI's computer systems is considered to belong to JMI and is recognized as part of its official data. It is therefore the responsibility of the users to exercise utmost care in sending/receiving information of confidential nature.
- The equipment, services and technology used to access the Internet are the property of JMI and the university in cases of inappropriate use are specifically brought to its notice reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the JMI email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by JMI if they are deemed to be harmful and/or not productive to business

- JMI reserves the right to limit the amount of download from Internet. This limit could vary for different user groups.
- In case of any legal issue arising out of use of ICT infrastructure misuse by the individual user, the university may take appropriate action and the user shall be responsible for such act.
- The user shall be responsible for keeping his/her account credentials safe and secure. Any hacking incident of email, MIS or any other official service must be immediately reported to FTK-Centre for Information Technology. JMI shall not be responsible for any misuse of the account subsequent to hacking.

Unacceptable use of the internet by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via JMI's email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization without obtaining prior permission of the owner.
- Hacking into authorized or unauthorized websites
- Sending or posting information that is defamatory to JMI, its products/services, colleagues and/or students
- Introducing malicious software onto the JMI network and/or jeopardizing the security of the university's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

E-Mail Usage

- **All employees on recommendations of their respective HoDs/Directors/Officers of JMI may be given an E-Mail account on jmi.ac.in domain.**
- Contractual employees my also be given email accounts, if their respective Heads of Departments/Directors of Centres recommend access to JMI's email for them. However, such recommendations must be accompanied with the declaration that the FTK-CIT will be explicitly informed for closure of such accounts once a contractual employee leaves JMI.
- The EMail usage will also be subject to the Acceptable Internet Usage policies
- All outgoing email shall have the following the following text appended to the email:

Password Security:

Appropriate security and access controls based on the criticality of the system must be implemented and enforced to protect passwords that provide access to network resources. The following password strength rules are minimum requirements that must be followed by the user and enforced as far as possible by the system for any system active on the University's network in which accounts are provided.

- **Encryption of Passwords:** All passwords stored on a system must be encrypted.
- **Format of Passwords:** The following format restrictions are designed to help prevent passwords from being compromised.
    - Passwords must be a minimum of 8 characters.
    - Passwords (with the exception of mainframe passwords) must incorporate at least 3 of the following: upper case, lower case, numbers, and special characters (i.e. punctuation and symbols).
    - Passwords must not include any portion of the user's logon name or the user's first or last name or a word commonly found in any dictionary.

Operating Systems/Network Applications:

System administrators are responsible for installing operating system and network applications updates of all manufacturer recommended security patches and for turning off all identified unnecessary services.

Virus Protection:

It is the responsibility of each user to ensure that an antivirus virus protection software is installed and enabled on his/her computers. Such AV software must be kept up-to-date by the user concerned. A scan of local storage must be scheduled to run minimally weekly.

Physical Security:

The physical security of the University's information technology resources (including, but not limited to the facility, equipment, software and information) must be maintained. Individuals and units are responsible for implementing security measures for the resources within their purview, commensurate with the criticality of each information technology resource.

All terms and conditions as stated in this document are applicable to all users of JMI's network. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by JMI.

Information about ICT equipment of non-consumable category purchased by the department or transferred from other departments of JMI must be maintained in the Departmental Stock Register which must be reconciled on yearly basis with the Central Stock register.

If an employee is unsure about what constituted acceptable Internet usage, then he/she may contact FTK-Centre For Information Technology, JMI.