

Sub: Policy for usage of email & internet

IOCL provides various facilities to its employees for improving the productivity of the employee such as PCs, Laptop, Internet Access, e-mail etc. on need basis. It is necessary that these facilities are used judiciously and for official purposes only. This internet usage policy has been designed keeping in mind enhanced PC penetration, the network security aspects and the need to avoid misuse/malicious use of internet.

Policy for allowing Internet Access:

1. Officers having networked PC will normally be provided e-mail facility. However, internet access will be provided to officers in grades "A" to "E" on need basis, on specific recommendation by HOD/location in charge in grade "G" and above.
2. Non-officer employees shall be provided e-mail on their PCs for specific purposes as certified by the Head of the Department and after due approval of the designated Competent Authority (Grade "H" and above).
3. E-mail account shall be closed immediately on the separation of the employee by way of Retirement, Resignation and Death etc.
 - 3a. Use of e-mail/internet facilities is prohibited for malicious activities like downloading of music/ video, playing music/ video, visiting pornographic sites & downloading pornographic pictures etc.
 - 3b. The server logs and the electronic 'paper trails' shall be considered proof for deciding misuse of e-mail and internet.
4. The internet communication should be preferably done using the corporate mailing system. The Fax messaging should be used only when the e-mailing is not possible.
5. Only System Administrators and officers in grade "H" & above shall be authorized to send mass mail. Any mail sent to a group of above 20 addresses shall be considered mass mail. However, some key officers, in other grades depending on need, shall be authorised by functional directors to send mass mails.
6. Internet user/ owner of an e-mail account shall be responsible for protecting his account and PC from unauthorized use. He/ She will take precautions in this regard. The owner of the e-mail account shall be held responsible, if his/ her account has been used to compromise the organisation, e.g. sending defamatory e-mail, use of harassment, unauthorized purchasing etc.
7. For all PCs on which internet access facility has been given should have a defined '**owner**', who could be held responsible for any violation of e-mail or Internet

usage policy from that PC. This would also apply to all user accounts who will be responsible for e-mail and Internet usage from their respective accounts.

8. Use of email is strictly prohibited in the following respects;
 - a. Sending or forwarding unnecessary messages or other non-work items particularly to several people.
 - b. Sending or forwarding material that could be construed as confidential to such recipients who are not authorized to receive the same.
 - c. Sending or forwarding political, profane, obscene, threatening, offensive or libellous emails.
 - d. Sending or forwarding messages for purposes constituting clear conflict of company interests and policies or violation of company's security policy.
 - e. Broadcasting unsolicited personal views on social, political, religious or other non-business matters.
9. In case any employee is observed to be violating above guidelines, his/her e-mail/ internet access will be barred without assigning any reason, besides appropriate action as deemed fit.
10. IOCL encourages the use of electronic mail and does not wish to inspect or monitor electronic mail routinely or to be the arbiter of its contents. Nonetheless, the electronic mail and data stored on the IOCL mail network of computers may be accessed by the Company or its authorized representative, for the following purposes:
 - Troubleshooting hardware and software problems
 - Preventing unauthorized access and system misuse
 - Retrieving business related information from an mail account
 - Complying with legal requests for information
 - Rerouting or disposing of undeliverable mail