## Internet Usage and Electronic Mail Policy

**Objective:**

To lay down the rules and regulations governing usage of HCL Technologies Internet Connectivity and E-mail facility for enhanced operational performance and adhering to legal, security and safety requirements.

**Scope:**

This Policy is applicable to all employees of HCL Technologies who access Internet and E-mail from their work premises, whether at HCL Technologies centers and offices or at on-site assignment locations/customer premises. This guideline is applicable to all systems under the jurisdiction and/or ownership of HCL Technologies, inclusive of hired systems.

**Need for Policy:**

- Loss of confidential data: Company sensitive information may leak out through E-mail, FTP or Newsgroup Communications.
- Potential Legal liabilities or negative publicity through inappropriate usage of Internet.
- Violation of software licensing laws by illegally downloading unlicensed software from Internet.
- Conduct of personal business using company resources.
- Visit to inappropriate sites allowing company domain to be captured, possibly resulting in negative publicity
- Loss of employee productivity: Management is concerned about the impact of non-business-related surfing on employee productivity and cost associated with wasted time/salary.
- Internet Access is not free. Non-business usage of Internet results in real costs to the organization- for example, the cost to upgrade network resources such as leased lines, routers, and disk storage to handle increased load.

**Internet:**

- Company provides access to vast information resources of the Internet to help the employees do their jobs faster and smarter and be a well-informed business citizen. Company in turn expects the employees to use these resources optimally.
- All existing company policies apply to their conduct on the Internet especially those that deal with intellectual property protection, privacy, sexual harassment, information, and data security.
- Each employee using the Internet facilities shall identify himself/herself honestly and completely when participating in chats, Newsgroups
- Any unauthorized downloaded software via Internet into the company's network is a legal liability to the company. Any such files / software may be used only in ways that are consistent with licenses or copyrights.
- Any unusual activity observed in Internet usage shall be reported as an Information Security incident.

**E-Mail:**

- The use of email systems must be related to business needs. Incidental or occasional personal use of email may occur when such use does not generate a direct cost for HCL Technologies.
- HCL Technologies is committed to respecting the rights of its employees, including their reasonable expectation of privacy. HCL will not monitor electronic mail as a routine matter, but it may to do so to

the extent permitted by laws, as HCL Technologies deems necessary for purposes of maintaining the integrity and effective operation of the electronic mail systems.

- To the extent permitted by law, HCL Technologies reserves the right to access and disclose the contents of user's electronic mail.
- Company reserves the right to intercept and filter out incoming attachments in e-mails, if found malicious and unauthorized.
- All messages generated on or handled by electronic communications systems, including back-up copies are the property of HCL Technologies and are not the property of users of the electronic communication services.
- Any unusual activity observed in E-mail usage shall be reported as an Information Security incident.

**E-mail Etiquette:**

- Write well-structured mails. Always include a short and descriptive and meaningful subject heading.
- Compress attachments whenever possible.
- Do not send unnecessary attachments.
- Clean up e-mails before forwarding them, so that the original idea is not hidden in obfuscation.
- Don't send or forward e-mails containing libelous, defamatory, or offensive remarks.
- Only mark emails as important/priority if they are important.
- Don't write emails in Capital letters.
- Include your name, job title, contact details in the signature.

**Undertaking on Information Security Policy Compliance**

**E-Mail Policy:**

I have read and understood the Company's Electronic Mail Policy. I fully understand the terms of this policy and agree to abide by them. I realize that the company's security software may scan and record, for management use, all mails I send and receive

**Internet Policy:**

I have read and understood the company's Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the company's security software may record the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive, for management use.

**Camera Usage Policy:**

I understand that photography inside Company's premises is not permitted through the usage of any device. Mobile phones and similar devices with cameras shall be utilized for voice communication and short messaging service purposes only.

**Removable Media Usage Policy:**

I understand that usage of any unauthorized removable media inside the Company's premises with the intent of copying information is strictly prohibited. Any violation could lead to dismissal or even criminal prosecution.

I am aware and accept applicable disciplinary actions, including dismissal or criminal prosecution, in case of violating the above policies.

**Software Asset Management**

I agree to abide by all terms and conditions always listed in the Software Asset Management (SAM) Policy. I will ensure that software will be installed on my machine only after I have received the requisite approvals for the same. I also agree to keep track of the software inventory on my machine(s), and to take necessary corrective actions if any installation is not in accordance with the SAM Policy. I further agree that the company will not accept any liability in respect of any unauthorized use of software and I shall be personally liable for any damages or other liability arising on account of violation of SAM policy.

*Note: Please refer to Global IT handbook on Policies Hub at myhcl.com for additional information*