Internet and Email facility - Conditions of Use

Guidance on 'Internet and Email facility - Conditions of Use' at HSBC Software Development (India) Private Limited

Misuse of e-mail, internet and the sending of text messages using HSDI equipment can have serious consequences (civil or criminal liability) for the staff. It is important that we try to minimize these risks. In general, information delivered electronically must be of an appropriate business nature. People tend to be more informal when using e-mail, the internet or when sending text messages to or from mobile devices. It is important that these conduits are used with same care as with any other correspondence. Do not routinely rely on the internet to guarantee delivery or content of messages. You must not use the internet for purpose of establishing or implying a contractual liability.

You must not create, view, download, send or forward, in any form and through any means of communication - any inappropriate material or action. This includes, but not limited to:

- Illegal, libelous, pornographic, sexually explicit or obscene images, racist images or messages; or other salacious or frivolous material
- Producing and sending of offensive messages where the content contravenes HSDI or HSBC Group's policy and which may defame, threaten, offend or harm an employee of HSBC Group and or / its affiliates, service provider, customer or anyone else
- Action prejudicial to another's business, their reputation or their internet access e.g. "Flaming" (publishing derogatory comments about a person) or "Spamming" (the internet equivalent of sending junk mail), which may embarrass the HSBC Group Company (including its affiliates) or damage its reputation or standing with customers, clients or anyone else
- Anything that is unethical or malicious or which may infringe copyright or other intellectual property rights
- Initiating or perpetuating "Chain" or "Pyramid" style correspondence

You must not, without specific prior approval from either your respective line manager or local IT support desk, obtain or purchase and download executable (.exe, .com) software, including, but not limited to the following:

- Music / Video files (MP3, MIDI, WAV, MPEG, Audio / Video Streaming etc.), including very large files (e.g. in excess of 5 Mbytes) that may take a long time to download
- You must not participate in news groups, user groups or any kind or type of chat rooms over the internet
- You must not, attempt to circumvent controls at any web site or service provider.

1. BUSINESS USAGE

Inbound & Outbound communication / exchanges - Virus scanning is carried out by default for all incoming and outgoing emails. However, you must not open files, messages or e-mail attachments without first ensuring that the sender is known to you. If a message is received from an unknown source or with a suspicious attachment, refer to the local IT support helpdesk. If you receive an unsolicited e-mail or attachments (including all "Chain" or "Pyramid" style) that you are suspicious about, then please refer or highlight the same to your respective manager / line manager to seek guidance and report the same.

For outbound communication / email exchanges containing restricted and highly restricted information must be encrypted. There is a potential risk that business communications could be intercepted and used in a manner that is damaging to the reputation of the HSBC Group. If the subject matter is both sensitive and confidential, please evaluate if you could use an appropriate alternative method.

Wherever applicable (example – regulatory reporting / submissions) you must ensure to save a copy of the email using appropriate retention strategy / methodology. If you are unsure whether or not to retain a copy, please contact your line manager for guidance.

I Agree and accept

Information Classification & labelling - All employees in HSDI or HSBC Group are responsible for properly identifying the classification of information and ensuring that it is handled accordance with this policy extract. All employees must adhere to controls, process and procedures in handling the information as defined by the HSBC Group. All employees must visibly label any new documents that they generate and any existing documents that they edit (e.g. Microsoft Office documents), and any new emails that they send with one of the four Information Classification categories as per Information Security policy of HSBC Group standards as enunciated below -

- **PUBLIC** - Information that poses an insignificant risk to HSBC, HSBC's customers and related parties. Its loss, corruption or disclosure will not result in regulatory/legal action, financial loss and/or damage to HSBC, HSBC's customers or related parties, and/or will not damage HSBC's reputation or business capability
- **INTERNAL** - Information that poses a minor risk to HSBC, HSBC's customers and related parties. Its loss, corruption or disclosure is unlikely to result in regulatory/legal action, financial loss and/or damage to HSBC, HSBC's customers or related parties, and/or is unlikely to damage HSBC's reputation or business capability
- **RESTRICTED** - Information that poses a moderate to major risk to HSBC, HSBC's customers and related parties. Its loss, corruption, or disclosure is likely to result in regulatory/legal action, financial loss and/or damage to HSBC, HSBC's customers or related parties, and/or is likely to damage HSBC's reputation or business capability
- **HIGHLY RESTRICTED** - Information that poses a massive risk to HSBC, HSBC's customers and related parties. Its loss, corruption or disclosure is highly likely to result in extensive regulatory/legal action, financial loss and/or damage to HSBC, HSBC's customers or related parties, and/or is highly likely to damage HSBC's reputation or business capability.

Restrictions - You must not use the Internet or @hsbc.com/@hsbc.co.in e-mail for the following purposes:

- Issuing any form of unauthorized business advice, or legal commitment by e-mail on behalf an HSDI or HSBC Group company
- Transmitting work-related documents across the internet that –
  - may result in a breach of current legislation. This includes confidential or sensitive information and data that can be attributed to any customer or employee of the HSBC Group.
  - contains information or data that may result in damage to the reputation or commercial dis-advantage of the HSBC Group if the information becomes public
  - concluded in any form of commercial or contractual agreement or of the communication of any advertising and marketing material without prior approval from HSBC Group Compliance

You are expressly forbidden from using or accessing "Web based" e-mail systems, such as "Hotmail, Yahoo, etc." POP3 accounts for business purposes, internet based instant messaging and peer to peer services

- Employees must not represent HSBC or share any HSBC Group information in internet discussion forums, social/career networks, news groups, chat rooms or similar platforms unless expressly justified and authorised by the relevant local business head. Records will be maintained of access to such forums etc via Group equipment and the strictures of GSM 8.4 Electronic Communications must be observed as must the Information Classification policy within the Security and Fraud section of the Operations FIM.

2. MONITORING

The use of e-mail and internet facilities for both personal and business purposes, and text messages sent to mobile phones using HSBC Group's equipment may be monitored, as may the content of attachments. Consequently, you cannot expect that using any of the Group's systems will remain absolutely private. The user will bear in mind at all times that electronic mail messages, however confidential or damaging, may have to be disclosed if at all raised out of a litigation scenario or a court proceedings or investigation.

I Agree and accept

- Usage of or access to the internet from HSBC Group premises (or equipment, wherever situated, made available by the HSBC Group) to employees of HSDI or HSBC Group companies or other permitted users is provided within the conditions laid down in GSM/FIMs and for business correspondence and is to be conducted in a business-like and professional manner. Use of email and external computer system access over the internet is provided for business matters only and is subject to the prevailing 'Internet policy', the Code of Conduct in force and is subject to consequence management up to and including revocation of access privileges and / or disciplinary action (including) cessation of employment

- Internet and email access is not to be used for the following purposes which are expressly forbidden: solicitation of correspondence unrelated to business activities, illegal, libelous or offensive messages, prejudice or harassment whether racial, sexual or of any other kind, action prejudicial to another's business, their reputation or their internet access (flaming, spamming etc.), for download of pornography, games software or other salacious or frivolous material, for obtaining or purchasing executable (.exe) software without specific prior approval or video, audio or music material, nor for participation in news-groups, use-groups or chat-rooms, nor for issuance of any form of formally unauthorized business advice, or legal commitment by email on behalf of any member of the HSBC Group, nor for the conclusion of any form of commercial contractual agreement; nor for communication of any advertising/marketing material without prior HSDI Local Compliance Office approval

- The user shall respect and abide by all applicable HSDI / HSBC Group policies, including confidentiality, copyright and data protection policies. In particular the user must not copy or transmit to third parties, the works of others without their permission as this may infringe copyright

- Hard copies must be taken of any electronic mail messages which need to be retained for regulatory or other legal purposes, as advised by the Compliance office

- The user must not import files or messages without ensuring that they have first been scanned for viruses. Please follow ISR guidelines or raise a ticket for technology support help desk

- The user will bear in mind at all times that electronic mail messages, however confidential or damaging, may have to be disclosed in case of court proceedings or investigations

- The relevant HSBC Group company/ies are entitled at any time to examine and/or download details of and/or monitor any usage of any kind by the user of the Internet including, without limitation, any email messages, whether or not created by the user, the content of any pages downloaded and any mechanisms which record the employee's use of the internet.

I accept the above notification along with its contents and agree to abide by the terms and conditions enunciated in this guidance document along with HSDI's standards norms, regulations and code of conduct in force as applicable.

Date: _____

Employee name: _____

_____

I Agree and accept