"GUIDELINES FOR STAFF ON USE OF IT FACILITIES"

Revolutionary ideas do not change institutions…
…People change them by taking the risks to serve and lead and by sustained painstaking care that institution building requires…

INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH,
Plot No 3, Sector - 18 A Dwarka, New Delhi-110075, INDIA.
(Dated 15th January 2021)

1. Terms of Use

These guidelines are issued by the Institute to provide clarification on the practical application of the Institute Policy on Acceptable Use of IT Facilities. These Guidelines apply to all staffs and students. Staff use of Institute IT facilities including email and the internet is conditional upon compliance with all Institute policies, procedures and guidelines.

2. Staff Conduct

2.1 Staff must adhere to the following rules:

Identity & Representation

- Provide evidence (e.g. a current staff ID card) of their eligibility to use the Institute IT facilities, on request from relevant Institute managers and concerned personnel.

Security of Facilities

- One should keep their username and password safe and not make their password available to others or use any account set up for another user or make any attempt to find out the password of a facility or an account for which they do not have authorised access.
- Ensure that the confidentiality and privacy of data is maintained.
- Ensure the security of their workstation by logging off or observing other security measures when it is left unattended.
- Be responsible for the safe keeping of the data they access as part of being granted access to use at Institute information systems.
- Report immediately to the IT Department if any breach of security pertaining to data from any information technology facility. Unauthorised release or use of data inadvertently obtained may lead to legal action.

Personal Use of Institute IT Facilities

- Ensure that IT facilities are utilised for the Institute teaching and learning, research, administrative and business activities that they are provided for.
- Ensure that personal use unrelated to work is limited, reasonable and appropriate and must not:
    - Contravene Institute Policy or under cyber laws,
    - Interfere with official use of IT facilities, or
    - Interfere with a staff member's obligations to the Institute.
- Recognise that the amount of personal use is at the discretion of a staff member's supervisor or manager and that advice should be sought from them before using the internet for personal purposes.

Advice

- Seek advice from their supervisor or the IT Department if they have doubt concerning their authorisation to use any IT facility or about whether a particular use is acceptable.

Email Bulletins & Notices

- Only send general notice bulletins to public groups, news groups, or specific work groups for the purposes of Institute business associated with work.

2.2 Staff must 'never' do the following:

Personal Profit

- Use Institute provided IT facilities for the purpose of personal profit making or for commercial activities other than those of the Institute.

Software

- Make use of, or copy, software contrary to the provisions of any licensing agreement entered into by the Institute. The onus is on staff to consult with concerned Department to clarify the permitted terms of use if they wish to use any software for purposes other than those for which the Institute has a licence.
- Install software on any Institute IT facility unless the installation is designated as part of their authorised work.
- Install Institute licensed software on any non-Institute owned facility unless the license specifically permits it.

Identity & Representation

- Represent themselves, in messages or otherwise, as someone else, fictional or real, without providing their real identity or username.
- Give the impression that the writer is representing, giving opinions or making statements on behalf of the Institute or any part of it unless appropriately authorised to do so via communications using Institute IT facilities.

Security of Facilities

- Divulge any confidential information that they may have access to in the normal course of their employment.
- Seek access to data that is not required as part of their duties as a staff member of the Institute.
- Behave in a manner which, in the opinion of relevant Institute managers and supervisors, unduly inconveniences other people or which causes or is likely to cause damage to Institute IT facilities.

- Store Institute data on personally owned devices or any other device not owned by the Institute where such device can be used by another person, unless such devices are locked down to the staff member via password, pin or biometric access and the device locks itself after no more than 5 minutes of inactivity

Personal Use

- Some types of unacceptable use, for example transmission of material of an obscene natures, are specifically prohibited by the Acceptable Use of Information Technology and by State and Cyber law. The policy contains an appendix listing relevant legislation and Institute policy and procedures.

3. Relevant Legislation

3.1 Copyright

Copyright law restricts the copying of software and other material subject to copyright (documents, emails, music, broadcasts, videos etc.) except with the express permission of the copyright owner. (The copyright of an email is owned by the sender, or the sender's employer.)

Email & Copyright

The copyright of an email message is owned by the sender, or the sender's employer. Copyright owners have a variety of rights, including the right to reproduce their work and the right of communication to the public. Forwarding something to an email discussion list would be construed as 'to the public'.

Consider the expectations of the originator:

- Did that person set any conditions on the further communication of their email?
- Expect that it would not be forwarded to anyone else? or
- Would not be forwarded to a particular recipient?

3.2 Privacy

A member of staff may expect some privacy in relation to their use of the computer and email and internet resources the Institute makes available to them at work. Despite the use of individual passwords, privacy is limited in the following ways:

- Use of computers, email and the internet as well as data on internet sites visited, downloads made and emails sent/received, can be accessed by IT administrators.
- It is possible to retrieve deleted records from back-ups and archives.

Privacy legislation.

Besides technological limitations on privacy, there are other factors that can impinge on privacy. The Office of the Privacy Commissioner provides information on the privacy

legislation and how it applies to use of IT by employees. It shows that there are exemptions to the Privacy Principles and an employer's logging of staff activities (email and internet) is not contrary to the legislation as long as it is done lawfully and fairly.
To ensure fairness, the Institute has provided these Guidelines to inform staff about its practice of monitoring and accessing records relating to the use of Institute IT facilities, including computers, email and the internet. The Institute also informs members of the public about how the Institute monitors their use of the Institute web site.

3.3 Information right

The Institute reserves the right to have access of staff official email if required with applicable login credentials. The content of these emails remains the property of the Institute.

3.4 Spam Act

All email messages sent from an Institute email account must comply with the Spam Act. This Act dictates the regulation of commercial e-mail and other types of commercial electronic messages.

The Spam Act makes allowance for the Institute, which is classified as an "educational institution", to send messages to current or previously enrolled students about its goods or services. Therefore, an 'unsubscribe' facility is not required in these cases. Other electronic messaging, including emails, instant messaging, SMS and other mobile phone messaging may be identified as spam if it does not fall into this category.

4. Alleged Misuse

Where an alleged misuse has been reported, the concerned person may:

- Act immediately to prevent any continuation of the alleged misuse pending an investigation.
- Promptly notify other authorities, including the relevant departments or individuals.
- Advise the staff member of the Acceptable Use of IT Facilities policy and direct the staff member to discontinue the alleged misuse immediately.

If an investigation of alleged misuse requires a staff members use of IT facilities to be examined or monitored they will not necessarily be notified.
Allegations that constitute misconduct or breaches of the law will be referred to the appropriate authority for investigation. The Institute may give that authority all reasonable assistance requested, including disclosing:

- Relevant data of the person which may be held by the Institute.

When misuse is observed:

- **If the incident is happening** report the incident directly to Institute concerned departments.

- **If the incident has happened** report the incident to the IT Help Desk.

4.1 Monitoring

Routine monitoring of the use of IT facilities is conducted to monitor the costs and acceptable use of Institute resources will take place. In normal circumstances, Institute and third party staff supporting IT services will not monitor the contents of electronic mail messages or other communications or files they access as a result of their work. However, the Institute and third party staff supporting IT services will inspect, copy, store and disclose the contents of email when appropriate to prevent or correct improper use, satisfy a legal obligation, or to ensure proper operations of IT facilities.

If any found to have visited porn or gambling websites or having access to obscene, anonymous, or any other material which are comes under cyber laws are subject to strict action against him accordingly.

Appendix A: Additional Information

To help staff use IT resources responsibly, the following information is provided:

Mailbox Management

- To maintain the performance and reliability of the Institute's email environment, size limits will be placed on the storage capacity for the on-line mailboxes for each user.
- All staff can reduce their storage demands by monitoring their storage usage, deleting unwanted mail or archiving email to other storage media (e.g. desktop drives, CD-R, DVD-R). Archiving will still permit easy access to material for retrieval. Institute recommends that staff liaise with their IT support staff to ensure that local conventions for archive storage are followed and appropriate backup procedures are undertaken.
- If staff do not receive emails for more than 24 hours, they must inform concerned department.
- Staff will receive system generated messages delivered to their mailbox informing them when they have reached their allocated quota and other technical message. One should inform the concerned department or help desk to sort out the problems.
- Staff are prevented from sending any more messages when they have reached 100% of their allocated quota. Staff have the option of removing and archiving items. Staff in this situation will not still continue to receive new messages.
- Staff are prevented from sending and receiving any more messages when they have reached 100% of their allocated quota. Staff have the option of removing and archiving items.
- Allocated quotas will be reviewed to ensure that 'normal' functions of staff can be performed within the quotas allocated.

When a Staff Member Leaves

- When a staff member's email account is to be deleted (because they are leaving the Institute), the person requesting the deletion must complete the appropriate formalities and have it authorised by the relevant Head of Concerned administration Department or Institute Director.
- It is the responsibility of the departing staff member to tidy up their email account prior to their departure. Messages which relate to Institute business should be retained or archived appropriately. Messages which remain in the email account will be viewed by other concerned authorized staff once the departing staff member has left if required.
- If messages arrive for a deleted email account in the three month period will not be automatically redirected to an email account. Personal mail messages for the former staff member will be on forwarded (if a forwarding e-mail address is known) on request of the departing staff member. Institute related e-mail messages will not be disclosed nor forwarded to the former staff member.
- Archived messages may be recovered for up to sometime by submitting a formal request to the IT Help Desk stating the reasons for recovery and the date/period of the mail messages to be recovered.

Use of Mailboxes:

- Mailboxes are provided as part of the email service. All requests for mailboxes must be approved by Concerned Departments
- Mailboxes are not to be used for archiving personal email data. Requests for mailbox to facilitate other purposes can be forwarded to the IT Department / concerned authority for consideration by individual. Requests for a mailbox must include:
    - the role or purpose of the mailbox
    - information detailing who requires access to the mailbox
    - the permissions for each person requiring access
    - the name of the designated owner for the mailbox for them to manage content
      and set access permissions
    - Approval by the reporting authority or concerned department as per the institute.

Use of Email Signatures

- Staff should include a signature file on all email. The signature should include the name of the sender, organisation, title, e-mail address, phone number, fax number and the institute URL
- An appropriate picture, graphic or link to promote your business unit, team or department or an upcoming institute event may be included in the signature block

however drawings, pictures, maps, graphics or an inspirational or other type of quotation are unnecessary in a business communication.

Restoration of email

- The restoration of a deleted email(s) will be provided only in special circumstances. A formal request needs to be submitted to the IT Help Desk, accompanied with an approval from a reporting authority. The formal request needs to stipulate the date the email was deleted, subject, sender of the email, recipient of the email and the reason that the email is required again.

Inadvertent Use

- In relation to use of the web, it may not always be possible to tell if a web page is relevant until it has been read and web search engines and links can sometimes lead to irrelevant and inappropriate websites. In these cases usage logs may be used to demonstrate that access to inappropriate sites was inadvertent.

All staff and student notices

If any staff or student regularly receives unwanted and unsolicited email received by staff or any other source, one should inform the concerned department for necessary action.

- Staff must not circumvent this by intentionally.

General Guidelines for Staff and Students at Computer Labs

Do's and Don'ts in the Computer Lab:

1) Eating of Food & Spilling of Tea, coffee and water or Wrappers is strictly prohibited
2) Usage of Cell phone is not allowed in Computer Lab. In case of emergency kindly leave the computer Lab and can talk in the corridor.
3) You are solely responsible for your personal belongings and the Institute is not responsible for any theft or damage to your personal Goods.
4) If any Computer Part is found damaged or missing from the Computer Lab then strict Action will be taken accordingly.
5) You are requested to arrange Chairs while seating or leaving the Computer Labs.
6) Please make an entry in the entry register of Computer Labs.
7) Sticking of Chewing Gums or any adhesive material if found is subjected to strict Action against the concerning person.
8) You are requested to maintain Silence and Decorum with in the Computer Labs.

In case of any support kindly ask the Lab officials.