NSHM IT Policy Charter

Document Number:	IT01
Name of Document:	NSHM IT Policy Charter
Applicability:	All NSHM Staff and Students
Document Owner	Executive Council
Document Status:	Approved
Date of approval:	6th July, 2020
Date last amended:	4th July, 2020
Date last reviewed:	5th July, 2020
Date of next review:	6th July, 2020
Related Documents:	*NSHM Online and Blended Teaching Certification Policy* *NSHM Digital Literacies Framework* *IT Facilities and Infrastructure Policy* *Teaching and Learning Plan 2020-2022* *Teaching and Learning Policy* *Scholarship of Teaching and Learning (SoTL) Good Practice Guide* *NSHM Privacy Policy* *NSHM Anti-Cyberbullying Policy* *The Information Technology Act, 2000* *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* *Contract Act, 1872*

1. Overview and Purpose

NSHM Knowledge Campus, Kolkata, Division of HGC Trust, Kolkata, (or 'The College') uses information technology (IT) to support business and higher education operations, teaching and learning, administrative and academic activity, student and staff record management, communications and data storage. This policy applies to NSHM staff and students.

2. Principles

The IT Facilities and Infrastructure Policy is integrated into NSHM operational structure in order to ensure the College integrates NSHM policy and Government of India legislation for cyber law and good practice within IT processes and procedures.

3. Roles and Responsibilities

The Executive Council is responsible for ensuring that IT resources, facilities and infrastructure are sufficient to maintain business and higher education operations and achieve strategic objectives. This includes reviewing and approving expenses for purchasing and improving IT resources.

The ITES Manager is responsible for monitoring, maintaining, and making recommendations for the improvement of all NSHM IT infrastructure. S/he is responsible for managing the use of NSHM IT resources, including physical infrastructure and activity that occurs on NSHM web servers, including communicating planned maintenance outages to staff and students, and ensuring access is restored quickly when unexpected outages occur.

4. Use of NSHM resources and facilities

All individuals who choose to use NSHM IT resources and facilities on campus or remotely, have a responsibility to act in a professional, respectful and lawful manner and in accordance with the relevant associated policies. **All staff and students at NSHM must read, be familiar with, and abide by NSHM policies.**

5. The NSHM Virtual Learning Environment

The NSHM Virtual Learning Environment (VLE) is a set of teaching and learning tools, platforms and applications designed to enhance a student's learning experience by including digital tools and processes and the internet in the learning process. IT Department is responsible for the maintenance and support for all components of the VLE.

6. IT Support

Staff and students have access to IT helpdesk support on-campus, online, via email and phone during campus open hours. Contact details for IT helpdesk support are available on the NSHM website, throughout the campus and via email.

7. Acceptable use of IT Facilities

- NSHM IT must be used in a lawful, ethical and responsible manner, and in accordance with applicable NSHM policies (listen above), and any additional terms of use that may apply to particular software or services.
- NSHM IT is provided for use in the academic, administrative, commercial and community activities of the NSHM. Some reasonable non-commercial personal use may be allowed, but as a privilege and not a right, and if that privilege is abused it will be treated as a breach of this Policy.
- Account holders must take all reasonable steps to protect their account from unauthorised use.
- Use of NSHM IT or "bring your own device" (BYOD) must not jeopardise the fair, secure, and productive IT environment of the NSHM community, nor the NSHM's operations, assets, data integrity or reputation.
- Users must not install or use unlicensed or malicious software on NSHM IT or BYOD, nor circumvent the NSHM's IT security measures.
- Users are expected to report actual or suspected breaches of this Policy or other security incidents that may be a threat to the security of NSHM IT in a timely manner.

8. Security of IT at NSHM

- NSHM will take all reasonable steps to protect the cybersecurity of NSHM IT, including its confidentiality, integrity, and availability.
- NSHM will implement and operate an information security governance framework in order to effectively manage the security of NSHM IT.
- The ITES Manager is ultimately responsible for the cybersecurity of NSHM IT. For NSHM IT resources not managed by ITES, the respective IT custodians are responsible for the implementation and management of this policy
- Where there is a threat to NSHM IT infrastructure or cybersecurity, or if the use of NSHM IT presents a risk to NSHM, the College may take any necessary action to mitigate the risks, with or without prior notice.
- Acquisitions of, and changes to, NSHM IT should not expose NSHM to unacceptable levels of information security risk.
- The cybersecurity of NSHM IT is maintained in order to protect NSHM's operations and information assets. Users should not use systems outside of NSHM IT to conduct NSHM business unless there is a genuine need to do so and such use is compliant with NSHM's protection guidelines.

9. Breaches of this Policy

Breaches of this Policy may result in suspension of access to NSHM IT and/or;

- In the case of NSHM employees, may constitute misconduct which will be addressed in accordance with the NSHM's Employer Agreement or relevant NSHM disciplinary procedures
- In the case of students, may constitute misconduct under the Student Misconduct Policy.
- Breaches of this Policy may also be reported to external parties as required under law.
- Failure to comply with this Policy or Policy Instrument may be considered as misconduct and the provisions of the relevant Policy or Procedure applied.

10. Further Information

If you have queries about NSHM's IT Infrastructure, or wish to make a complaint, please contact the NSHM ITES Department or by email to ites@nshm.com in the first instance.

11. Accountabilities and Responsibilities

The Executive Council is responsible for this policy. NSHM will ensure students and staff receive information about this policy as part of their induction or orientation to NSHM.

12. Policy review

This policy will be reviewed by the Executive Council as required.

Haricharan Garg Charitable Trust ★ 124, B. L. Saha Road ★
Kol- 53

NSHM

Knowledge
Campus

IT Policy

Notes on this Policy

1. The term “NSHM” in this policy refers to the common brand and management organization of all educational campuses operating under the legal structure of their respective trusts.
2. This policy replaces any or all earlier IT Policies in the organization and will be in force from January 01, 2010.
3. It applies to all NSHM locations and all NSHM Team Members.
4. This policy is not applicable to Students. A separate policy will be issued for them. Till such time students will be governed by the provisions made in the Student’s Handbook and the Campus-specific Computer Centre rules.
5. Prepared by: Sanjay M Patel, Deputy Director-ITES, NSHM Knowledge Campus; approved by: the Chief Mentor

Date of Release: December 22, 2009

I. STATEMENT OF PURPOSE

NSHM provides networked computer systems, electronic mailing resources, and internet connectivity to support its operations. This administrative policy statement sets forth NSHM's policy with regard to use of, access to, storage and retrieval of information with the objective of ensuring that its resources are used to serve the above stated purpose only.

II. INTRODUCTION:

1) This policy covers the use of all NSHM-provided computer systems & facilities including access to the Internet and Electronic Messaging. The policy applies to all permanent, contract, and temporary Team members and persons affiliated to NSHM who use these facilities.
2) The policy defines what constitutes acceptable and unacceptable use of all IT resources mentioned in clause 1 above.
3) NSHM’s computer systems are important NSHM resources and are provided to Team members for efficient processing, storage and exchange of information and data pertaining to their assigned responsibilities and services.
4) Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that wastefully or non-productively use computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-work related uses of the Internet.
5) Users of NSHM provided computer systems are advised that there are no facilities provided by NSHM for the storage of any private, personal or confidential data or files. NSHM appointed IT administrators may have access to all data, messages, and files, and monitor all usage as necessary to assure efficient performance and appropriate use.
6) Team members are required to report any violation of this policy by themselves or others, immediately to their supervisor, or to the Systems Administrator.

III. Use of NSHM provided computer systems.

NSHM computer systems include all hardware, software, data communications, and integration thereof, that has been provided by NSHM.

All software purchases financed by NSHM for department specific use, are NSHM resources & need to be deposited with the IT department together with their security keys for cataloguing prior to their installation.

A. Privacy, Confidentiality and Public Records Considerations

All files and information stored in NSHM provided computers would be the property of NSHM and therefore will constitute public records accessible to authorised NSHM personnel and subject to public inspection under the Law of the land.

B. Permissible Uses of the Computer System

1) Authorized Users

Each Computer System (desktop/laptop) and its login will be assigned to one Team member, who would be the authorised user of the system, responsible for its use and upkeep, for keeping it secure, and for proper organisation of files and information stored therein.

All new and existing authorised users of NSHM provided Computer systems and facilities will take full responsibility of their systems by signing the last page of this policy and returning it to HR/IT department.

Certain systems out of the above may be designated group/departmental systems by their respective heads to be accessed by the authorised user with responsibilities as above as well as other Team members (secondary users) nominated by the group/department head.

NSHM discourages the practice of Team members bringing in personal laptops to work.

2) Purpose of Use

The use of any NSHM-provided computer system must be related to NSHM work.

3) Permissible Use & Related Responsibilities

a) Each machine will be assigned the Authorised User's Name (which will act as the Computer Name).

b) All users will be assigned general Windows user accounts. These accounts do not have any administrative or software installation rights.

c) Software Access Procedure : Software needed, in addition to the Microsoft Office suite of products, must be authorized by the department head and installed by the IT department only. Team members needing access to software, not currently on NSHM network, shall talk with their supervisor and the IT department.

d) NSHM appointed IT administrators are responsible for loading anti-virus software. However, the authorised user has to ensure this is updated regularly. It will be the user's responsibility to keep his/her computer system virus free.

e) System Users need to respect the legal protection provided to programs and data by copyright and license.

f) NSHM will make reasonable efforts to provide prompt maintenance support for the computer systems it provides to its Team members, but users are primarily responsible for its upkeep. Because of the nature and technology of computer systems, NSHM cannot assure either 100% uptime of its systems or 100% protection from loss of data/information stored on the system. Users are therefore advised to regularly backup their data on alternate back-up facility provided by NSHM.

g) Authorised users are required to store all their files & folders under one User folder tree only, preferably in D: drive in a multi-partitioned system, in order to facilitate regular backup of data in the system.

h) Authorised users shall safeguard their personal NSHM provided email accounts and single user passwords by changing them at regular intervals. Passwords for Windows, Outlook and official email IDs will have to be shared with IT representatives as and when requested. It may be changed by the user again thereafter.

i) Team members may encrypt data, messages and files only with software approved by NSHM. NSHM may require a copy of any decryption key necessary to access encrypted data, messages or files, as well as the password used for this purpose by an Team member.

C. Prohibited Uses of Computer Systems

1) Prohibited Purposes

a) Personal use that creates a direct or indirect cost for NSHM is prohibited.

b) NSHM's IT Systems shall not be used for personal monetary gain or for commercial purposes that are not directly related to the work/business of the organisation.

2) Other Prohibited Uses : Other prohibited uses of Computer Systems include, but are not limited to

a) Obtaining or securing Administrative rights to the Computer System. Administrative rights for all computers – desktops and notebooks, will be held by the IT department only.

b) Storing any data or files whose content could be considered illegal, offensive, fraudulent or defamatory. This includes any image or text that is pornographic, racist or discriminatory.

c) Storing or installing any copyrighted images, software, or text belonging to third parties without the copyright-holder’s permission.

d) Using USB pen drives, CDs/DVDs or similar devices for storing important NSHM data and carrying this outside NSHM premises.

e) Attempting to read, delete, copy or modify the data or files of other users without the permission of the user or the department head.

f) Transmitting NSHM or client information to third parties unless NSHM has expressly directed or granted permission to do so.

g) Spending inappropriate amounts of time during the working day using NSHM provided computer systems for personal use.

h) Creating shares of files & folders with other systems on the network on a permanent/long-term basis. (Shares facilitate faster propagation of viruses over the network).

D. NSHM Access and Disclosure

1) General Provisions

a) NSHM owns all data, information & files stored in computers provided by it. Please do not consider any of these to be private.

b) NSHM reserves the right to access and disclose the contents of its computer systems without the consent of the user. NSHM will do so when it believes it has a legitimate need including, but not limited to, those listed in paragraph D3 (below), and only after explicit authorization is obtained from the appropriate NSHM authority. To this end passwords for MS Outlook & official email IDs will have to be shared with the IT representative as and when requested.

c) Users are advised that the files in their computers should be treated like records of NSHM’s internal & external transactions and therefore as a shared filing system, i.e., with the expectation that these shall be made available for review by any authorized NSHM official for purposes related to NSHM work.

d) Any user who makes use of an encryption device to restrict or inhibit access to his or her files must provide access to such encrypted data when requested to do so under appropriate NSHM authority.

2) Monitoring of data / files stored

NSHM will not monitor stored data/files as a routine matter but it may do so to the extent NSHM deems it necessary for purposes of maintaining the integrity of its records and for efficiency/effectiveness of the operations of NSHM.

3) Inspection and Disclosure

NSHM reserves the right to monitor, inspect and disclose the contents of any computer system:

a) in the course of an investigation triggered by indications of misconduct or misuse, but will endeavor to inform an affected Team member when this is to happen and the reason for it
b) as needed to protect the health and safety of the system, and to maintain continuity of its operations
c) as needed to prevent interference with achievement of NSHM goals, or
d) as needed to locate substantive information required for NSHM work that is not more readily available by some other means e.g. if the Team member is absent for any reason and stored documents are required to be accessed for smooth running of the operation.

NSHM will inspect and disclose the contents of IT Systems when such action is necessary to respond to legal processes and to fulfill NSHM's obligations to third parties.

E. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of NSHM's IT resources. Disciplinary actions range from verbal warnings to termination, including possible civil and/or criminal liability. The severity of the misbehaviour governs the severity of the disciplinary action.

F. Retention and Archiving of all Files & Folders

NSHM appointed IT administrator(s) are responsible for taking backups of data from all desktops & laptops at regular intervals. In case of important data/information, user will be responsible to have the backup taken whenever required.

IV. Use of the Electronic Messaging System

Electronic Messaging includes e-mail, instant messaging, text messaging, fax, voicemail and any integration thereof. NSHM will allocate email-id’s to approved team members in the standard naming convention being followed only.

A. Privacy, Confidentiality and Public Records Considerations

NSHM will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, NSHM can assure neither the privacy of an individual user's use of its electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

In addition, communications of NSHM personnel that are sent by electronic mail would constitute "correspondence" and, therefore, will be considered public records subject to public inspection under the Law of the land.

B. Permissible Uses of Electronic Mail

1) Authorized Users

Only NSHM staff and other persons who have received specific permission from HR are authorized users of the electronic mail systems and resources.

Only Executive Council members and Campus HR heads are authorised to send bulk mails or mails to large groups of team members.

2) Purpose of Use

The use of any resources for electronic mail must be related to NSHM work. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for NSHM. Any such incidental and occasional use of electronic mail resources for personal purposes is subject to the provisions of this policy. This is not to be treated as a matter of right. The user will be responsible for appropriate use of the mail-id which depicts the name “nshm” and must not in any way let any kind of misuse of this medium adversely affect the image of NSHM.

C. Prohibited Uses of Electronic Mail

1) Prohibited Purposes

a) Personal use that creates a direct cost for NSHM is prohibited.
b) NSHM's electronic mail resources shall not be used for personal monetary gain or for commercial purposes that are not directly related to its work.

c) Originating or circulating any other unlawful matter with libelous, defamatory or discriminatory contents.

2) Other Prohibited Uses : Other prohibited uses of electronic mail include, but are not limited to

a) Sending copies of documents in violation of copyright laws
b) Inclusion of the work of others into electronic mail communications in violation of copyright laws.
c) Sending large files (larger than 2 MB).
d) Capture and "opening" of electronic mail except as required in order for authorized Team members to diagnose and correct delivery problems.
e) Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct NSHM work e.g.

- sending abusive, offensive or illegal material
- sending racist or otherwise defamatory communications
- sending or receiving emails that are detrimental to NSHM
- sending pornographic jokes or stories via email (this is considered sexual harassment and will be addressed according to our sexual harassment policy)

f) Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.
g) "Spoofing," i.e., constructing an electronic mail communication so it appears to be from someone else.
h) "Snooping," i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial NSHM purpose.
i) Initiating or forwarding Chain mails – Chain mails use up a disproportionately large quantum of

- mailbox & system storage space
- communication bandwidth

j) Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.

E-mail requires extensive network capacity. Sending unnecessary e-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical NSHM operations. When NSHM grants an individual Team member access to the network, it is the responsibility of the Team member to be cognizant and respectful of network resources.

D. NSHM Access and Disclosure

1) General Provisions

   a) NSHM owns any communication sent via email or that is stored on NSHM equipment. Please do not consider your electronic communication, storage or access to be private if it is created or stored at work and/or using your nshm mail-id.

   b) NSHM reserves the right to access and disclose the contents of users' electronic mail without the consent of the user. NSHM will do so when it believes it has a legitimate need including, but not limited to, those listed in paragraph D3 (below), and only after explicit authorization is obtained from the appropriate NSHM authority. To this end passwords for MS Outlook & official email IDs will have to be shared with the IT representative and as and when requested.

   c) Users are advised that NSHM's electronic mail systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on NSHM work or with the use of NSHM resources may be made available for review by any authorized NSHM official for purposes related to NSHM operations.

   d) Any user of NSHM's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate NSHM authority.

2) Monitoring of Communications

NSHM will not monitor electronic mail as a routine matter but it may do so to the extent NSHM deems necessary for purposes of maintaining the integrity and effective operation of NSHM's electronic mail systems.

3) Inspection and Disclosure of Communications

NSHM reserves the right to monitor, inspect and disclose the contents of electronic mail:

   a) in the course of an investigation triggered by indications of misconduct or misuse, but will endeavor to inform an affected Team member when this is to happen and the reason for it,

   b) as needed to protect its health and safety,

   c) as needed to prevent interference with achievement of NSHM goals, or

   d) as needed to locate substantive information required, that is not more readily available by some other means e.g. If the Team member is absent for any reason and communications must be checked for smooth running of day-to-day operations.

NSHM will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill NSHM's obligations to third parties.

4) Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring

The contents of electronic mail communications, properly obtained for NSHM purposes, may be disclosed without permission of the user. NSHM will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve an academic purpose or satisfy a legal obligation.

5) Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail Communications

   Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must obtain approval in advance of such activity from the appropriate NSHM authority.

E. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of NSHM's electronic mail resources. Disciplinary actions range from verbal warnings to termination, including possible civil and/or criminal liability. The severity of the misbehaviour governs the severity of the disciplinary action.

F. Retention and Archiving of Electronic Mail

Electronic mail messages containing decisions, procedures, operations, organization, functions, policies, or other activities of NSHM must be segregated, retained, and archived by recipients at regular intervals, in compliance with NSHM policy.

V. Use of NSHM Provided Internet Facility

Internet facility includes internet browsing, internet chat, VOIP communications, ftp, upload or download of files & information etc. and any integration thereof.

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content.

Internet use brings the possibility of breaches to the security of confidential NSHM information. Internet use also creates the possibility of contamination to our systems via viruses or spyware. Spyware allows unauthorized people, outside NSHM, potential access to NSHM passwords and other confidential information.

Removing such programs from NSHM network requires IT staff to invest time and attention that is better devoted to productive work. For this reason, and to assure the use of work time appropriately for conduct of NSHM work, we ask staff members to limit Internet use.

To minimize these risks, your use of the Internet at work is governed by the following policy:

Disclaimer

Users accessing the internet do so at their own risk and NSHM is not responsible for material viewed or downloaded by users from the Internet.

A. Privacy, Confidentiality and Public Records Considerations

Because of the open nature and technology of the internet, NSHM can assure neither privacy nor confidentiality of users visits to websites hosted on the internet or of communications in chat rooms etc.

In addition, logs of user’s visits to all websites will be considered public records subject to public inspection under the Indian Law.

B. Permissible Uses of the Internet

1) Authorized Users

Only NSHM staff and other persons who have received specific permission from HR are authorized users of NSHM provided Internet resources.

2) Purpose of Use

The use of the internet at work must be related to NSHM work. Incidental and occasional personal use of the internet may occur when such use does not generate a direct cost for NSHM. Any such incidental and occasional use of internet resources for personal purposes is subject to the provisions of this policy.

3) Permissible Use

   a) Researching the internet for academic & related support purposes.
   b) Files which are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions must be taken by the user to detect a virus/malware/spyware and, if necessary, to prevent its spread.

C. Prohibited Uses of the Internet

1) Prohibited Purposes
   a) Personal use that creates a direct cost for NSHM is prohibited.
   b) NSHM's internet resources shall not be used for personal monetary gain or for commercial purposes that are not directly related to its work.
2) Other Prohibited Uses : Other prohibited uses of the internet include, but are not limited to
   a) Private, non-NSHM related purposes such as marketing or private advertising of products or services or any activity to foster personal gain
   b) Downloading of software, shareware, music, movies, pictures, images, MP3, WMA files etc.
   c) Downloading material protected under copyright law or making that material available to others for copying. Team members are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material.
   d) Installation of software downloaded from the internet
   e) Chatting during work hours
   f) Gaming and gambling online or offline
   g) Subscribing to stock or news tickers of any kind resulting in consumption of internet bandwidth of NSHM
   h) Accessing streaming audio and/or video files
   i) Hacking (the unauthorized attempt or entry into any other computer).
   j) Sending or posting any NSHM material or information on any publicly accessible Internet computer without prior permission.

k) Alternate Internet Service Provider connections to NSHM’s internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

D. NSHM Access and Disclosure

1) Monitoring of Usage

NSHM will not monitor internet traffic as a routine matter but it may do so to the extent NSHM deems necessary for purposes of maintaining the integrity and effective utilisation of NSHM's internet bandwidth.

2) Inspection and Disclosure

NSHM reserves the right to monitor & inspect internet usage by its Team members as well as disclose these details whenever necessary.

3) Blocking Sites With Inappropriate Content

NSHM reserves the right to utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

E. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of NSHM's internet resources. Disciplinary actions range from verbal warnings to termination, including possible civil and/or criminal liability. The severity of the misbehaviour governs the severity of the disciplinary action.

F. Retention and Archiving

Not Applicable

VI. Disclaimer

1) NSHM reserves the right to change its IT policies and rules at any time.

2) This policy is intended to be illustrative of the range of acceptable and unacceptable uses of NSHM IT systems and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement should be directed to the HR/IT department.

3) NSHM will review alleged violations of the IT policy by all users on a case by case basis. Violations of the policy will result in disciplinary actions and/or use of local law depending on severity.

VII. Team member Acceptance

NSHM IT Systems, Electronic Mail & Internet Policies

Department : _________________________ User Name : _________________________ Computer /Account Name : _____________	Department Head : ____________________ User Type : Authorised / Secondary

I have read and understand the System, Email & Internet Policies listed above. By signing this form, I agree to abide by these policies currently in place and I agree to review them periodically for any changes or modifications. I recognize that the law and associated policies regarding the use of NSHM's Systems, Electronic mail and the Internet are continually evolving. Therefore, I understand that my regular review of policy is required.

I understand that team members are given these resources to assist them in the performance of their jobs. Team members therefore should have no expectation of privacy in anything they create, store, send or receive using NSHM's computer equipment. The computer network is the property of NSHM and may be used only for NSHM purposes.

Waiver of privacy rights : I therefore expressly waive any right of privacy in anything I create, store, send or receive using NSHM's computer equipment or Internet access. I agree to allow NSHM personnel access to and review of all materials created, stored, sent or received by me through any NSHM network or Internet connection.

Report Violations : I undertake to report any violation of this policy by myself or others, immediately to my supervisor, or to the Systems Administrator.

Team Member Signature:____________________________________ Date:_____________

Department Head Signature:_________________________________ Date:_____________

[To be included in Team member's personnel file]