



NAHANYATE FOUNDATION

(A duly registered trust for charitable purpose)

NAHANYATE FOUNDATION

(A duly registered trust for charitable purpose)

SONAJHURI (JHARNATALA), KHOAI
SANTINIKETAN, BIRBHUM - 731236
WEST BENGAL

+ 91 77193 69824

nahanyatefoundation@gmail.com

IT Manual



Table of Contents

Objective.....	3
Purpose.....	3
Advantage	4
Management Responsibility	4
Computer Internet Usage Policy Procedure.....	4
E Management Guideline.....	5
Software Policy	5
Information Technology Security Policy	6
Website Policy.....	6
Conclusion.....	7



1. Objective

This policy manual is designed to provide accurate and timely information on NAHANYATE FOUNDATION policies relating to IT Compliance with various centres of NAHANYATE FOUNDATION. The IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business/centres.

NAHANYATE FOUNDATION will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all members of NAHANYATE FOUNDATION.

The manual is intended to provide policies and procedures with links to more detailed information and guidance on the application of NAHANYATE FOUNDATION policies, practices, and procedures located on the Information Technology Compliance and other applicable areas.

All the Divisional Heads should provide direction to their staffs to ensure consistent application within each department accordingly.

This manual contains a set of basic performance expectations for administrators and staff. Departments can create unit -specific expectations based on operational needs and these should be communicated to employees. All employees are expected to perform at a high level consistent with their job responsibilities, represent NAHANYATE FOUNDATION in a manner consistent with our Brand Image.

The policies and benefit plans referred to in this policy manual are intended to be ongoing, however, NAHANYATE FOUNDATION reserves the right to amend, modify or terminate these plans at any time. If there are any discrepancies between the information contained in this policy manual and the legal plan documents, which describe the plans in detail, the plan documents will prevail. Changes in benefit plans and/or policies will be communicated through publications such as verbal/written or e-mail correspondence to members.

The IT policy manual covers the common IT requirements and practices. The IT manual establishes and states the policies governing NAHANYATE FOUNDATION IT standards and practices.

The purpose of this Information Technology (IT) manual is to define, develop, and document the information policies and procedures that support organizational goals and objectives. The policies and procedures provide:

- A foundation for a system of internal controls
- Guidance in current Computer and Network activities
- Criteria for decisions on appropriate IT security

These policies and procedures assure that the information assets are protected from a range of threats in order to ensure business continuity and maximize the return on investments of business interests. All additional departmental or functional policies and procedures written should conform to and parallel the policies in this manual. All changes to policies and procedures are required to be reviewed to ensure that there are no conflicts with the policies stated in this IT PolicyManual.

2. Purpose

It is intended to serve in defining, understanding and communicating our standard policies and procedures, identifying responsibilities, and providing guidelines in the performance of specific tasks. The content of this manual should address broad policies that impact across the entire institution. The policies



and procedures contained in the IT Manual are those policies and procedures of NAHANYATE FOUNDATION which are unique to NAHANYATE FOUNDATION.

3. Advantage

The main benefits of having this policy and procedure manual:

- Ensures all staff are aware of obligations in relation to selection, use and safety when utilizing information technology within the business.
- Helps give each employee a clear understanding as to what you expect and allow.

4. Management Responsibility

- IT Organization
- Planning
- Responsibility, Authority, And Communication
- Management Reporting
- Business Conduct

5. Computer Internet Usage Policy Procedure

The Computer Internet Usage Policy Procedure delineates procedures for accessing IT network of NAHANYATE FOUNDATION.

The Company Internet Usage Policy Procedure applies to all personnel with access to Internet and related services including but not limited to electronic mail (email), File Transfer Protocol (FTP), Gopher, and World Wide Web access.

Access to the Internet is specifically limited to activities in direct support of official company business. In addition to access in support of specific work related duties, the company Internet connection may be used for educational and research purposes. If any user has a question of what constitutes acceptable use he/she should check with their supervisor for additional guidance.

Computer Internet Usage Responsibilities: All Employees are responsible for knowing and adhering to this usage policy.

- Computer Internet Usage Policy Procedure Activities:** Acceptable Use-Computers and Internet. Internet can be used only for official, education or research purpose. It cannot be used for personal use. Only checking of personal e-mail is allowed.

E-mail Etiquette

- a) Official communications need to be made from official e-mail id only.
- b) Anybody using any official e-mail id needs to ensure the security of that id.
- c) No personal e-mails can be routed through official e-mail id.
- d) No personal e-mail should be there in the official e-mail.

Computer and Internet Usage-Security

- a) Firewall security will be there for restricting unwanted sites in the official domain.
- b) Social networking and restricted sites should be blocked in all the machines with internet connectivity



- c) Computer and Internet Usage-Penalties
- d) Failure in maintaining internet usage guideline will lead to strict disciplinary action. For severe violation of policy will lead to dismissal.

6. E-Management Guideline

- Hard copy paper work needs to be reduced and maximum official work needs to be done online.
- It is the responsibility of the section heads to develop software's in-house required for day to day operation of the department.
- For Employee Details, Salary Details, Payments Details online database needs to be maintained.
- Salary needs to pay online.
- Trust is aiming to migrate to "Cloud Computing" in the near future.
- For intra office communication intranet needs to be used.

7. Software Policy

This policy provides guidelines for the use of software for all employees within the business to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

We use only legal software for training. Refer to the copyright agreement of individual software before installation. Existence of illegal software will lead to immediate termination of our franchisee contract. Refer to detailed guidelines provided by NASSCOM in this regard. Suffice it to mention here that software piracy is a non-bail able offence with a minimum imprisonment of 6 months.

i. **Software Licensing**

- Software licenses terms and conditions will be followed by all employees of the Institute.
- Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of the section head to ensure these terms are followed.

ii. **Software Installation**

- All software must be appropriately registered with the supplier where this is a requirement.
- Only software obtained in accordance with the getting software policy is to be installed on the business's computers.
- All software installation is to be carried out under supervision of section head.
- A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

iii. **Software Usage**

- Only software purchased in accordance with the getting software policy is to be used within the business.
- Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.
- All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately.



- Employees are prohibited from bringing software from home and loading it onto the Institute's computer hardware.
- Software cannot be taken home and loaded on a employees' home computer
- Unauthorized software is prohibited from being used in the Institute .This includes the use of software owned by an employee and used within the Institute.
- The unauthorized duplicating, acquiring or use of software copies is prohibited.

iv. **Breach of Policy**

- Where there is a breach of this policy by an employee disciplinary action will be taken against the employee.
- Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify to section head immediately.

8. **Information Technology Security Policy**

- i. **Procedures for Physical Security:** All security and safety of all IT related devices like Desktop; Laptop etc. will be the responsibility of the employee who has been issued with these devices. Each employee is required to use locks, passwords etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, section head will assess the security measures undertaken to determine if the employee will be required to reimburse the Centre for the loss or damage.

All devices as laptop, notepads, iPads when kept at the office desk is to be secured lock, password etc.

- ii. **Procedures for Information Security:** All sensitive, valuable, or critical Centre data is to be backed-up.

It is the responsibility of System Admin/Technical Head to ensure that data back-ups are conducted on regular interval the backed up data is kept in proper places.

All technology that has internet access must have anti-virus software installed. It is the responsibility of System Admin/Technical Head to install all anti-virus software and ensure that this software remains up to date on all technology used by the Institute.

9. **Website Policy**

The website register must record the following details:

- List of domain names registered to the centre
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting
- The content of the website is to be reviewed on regular basis
- Only authorized persons are allowed to make changes to the Centre website.



10. Conclusion

The purpose of this IT Compliance Manual in general is to serve as training material and a guide as per the Quality norms of NAHANYATE FOUNDATION. In addition, an important purpose is to ensure consistency. Procedures are designed to help reduce variation within a given process clearly stating the purpose that helps gain employee cooperation, or compliance, and will instill in our employees a sense of direction and urgency. The Manual has been designed keeping in mind the mission, vision and objective of NAHANYATE FOUNDATION. So, everyone working in this Trust has to abide by the same for betterment of self and Trust in a broader perspective.

Employees are expected to acquaint themselves fully with the contents of this manual in order to establish and follow the procedures as exactly mentioned in this document. Since it is the policy to encourage employee participation in all matters that affect their work, employees are encouraged to offer suggestions for improvement to these policies and guidelines.