SNDT Women’s University

Information Technology (IT) Policy

(This policy has been approved by the Management Council)

I. Preamble:

Information Technology (IT) Policy of SNDT Women's University Technology sets out the core policies for the procurement, responsible use, maintenance, storage and disposal of the various IT assets and IT service of the University. This refers to IT facilities allocated centrally on its campuses or to the different departments/institutes/colleges. It is expected that all members of the University will be aware of and abide by this policy. Users of the campus network, computing resources and IT services are responsible for the appropriate use and protection of information resources and respect for the rights of others.

II. Definitions:

Information Technology (IT):

Information Technology (IT) refers to the technology (digital processes and devices) used for data gathering, processing for information generation, further processes on information for various outcomes, and retrieving information in digital formats.

IT Infrastructure:

It includes electronic infrastructure available for campus users and services, information available for external intended stakeholders for various official and academic purposes.

III. Scope:

The IT Policy is applicable to all university faculty, staff, students and all others using the IT resources. This includes all university owned, licensed, or managed hardware /software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

IV. Objectives of the Policy:

- To ensure that all the users of the University are responsible for adhering to the procedures governing the implementation of this Policy document and any other matter incidental to those rules
- To ensure that use of IT Systems is consistent with the principles and values that govern use of other University facilities and services
- To ensure the integrity, reliability, availability, and superior performance of the University IT assets

V. Policy Sections:

a. Appropriate use of IT Assets

- The users of the University shall use campus collaboration systems, internet, wireless resources, official websites and portals, Management Information Systems (MIS), ERP solutions, Learning Management System, Remote Login based facilities of the University and e-Library resources for the authorized purposes – that is, to support the research, education, clinical, administrative, and other functions of the University.
- The University shall stress upon the users to comply with University policies and legal obligations (including licenses and contracts).
- Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of the University shall be avoided.
- Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy.
- University should encourage use of Free and Open Source Software for various processes. Use of pirated software is strictly not allowed.
- Users must abide by the rules of the University towards the usage of social networking sites, mailing lists, newsrooms, chat rooms and blogs. Access to sites that are banned under law or that are offensive or obscene is prohibited.
- The University IT resources shall not be used for any commercial and promotional purposes, through advertisements, solicitations or any other message passing medium, except as permitted under University rules.

b. Security and Integrity

- The university IT resources should not be used for activities violating the basic functionality and mission of the University.
- The users must refrain from making any unauthorised access of information in order to promote secure access of Network and Computers.
- The Computer Centre has the right to monitor and scan all information carried by the network for the purpose of detecting and identifying inappropriate use. The competent system administrator may access the information resources for a legitimate purpose.
- A secured flow of internet and intranet traffic in the campus shall be managed through the firewall. Security related to digital devices is to be ensured with Passwords, Access Rights, Backups, Anti-Virus Measures, use of external media and so on. Physical Security will be ensured by securing parts of physical location to regulate its access, to restrict only authorized personnel, to provide for smoke detectors and fire alarms, to enable monitoring through CCTV Cameras.
- Anyone who has observed, has knowledge of, or has been the victim of any improper or prohibited use of IT assets is encouraged to report such activity by contacting the University Computer Centre and the appropriate university authorities.
- The regular updating of the anti-virus policy and security updates should be done for the protection of computing resources.
- University shall take proactive steps to reduce the risks associated with the sharing of the institutional information to a third party.

c. IT Asset Management

- The University shall lay down procedures for the management of hardware and software assets that facilitates the usage of IT resources in the University. This shall include procedures for managing the purchase, deployment, maintenance, utilization, energy audit, and disposal of software and hardware applications within the University.
- The University shall develop standard procedures for identification, minimization and monitoring of risk impact by preventive and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate

internet connectivity for a fail-safe internet access.

- The university must earmark an adequate budget for maintenance of the existing IT infrastructure. Dedicated IT maintenance staff is to be recruited to maintain and monitor existing IT infrastructure and networking.
- The University shall ensure that there is no violation in the copying and distribution of proprietary and licensed software applications.
- The University shall endeavor towards the promotion and effective usage of open source software applications.
- The disposal of hardware equipment shall be done as per the eWaste Management policy of the university.
- There must exist a system of cross checks and physical verifications of IT Assets to ensure that all assets exist, they are functioning as expected, are technically fit and not obsolete.
- Periodical audit of campus network, electric network and centalised IT infrastructure should be done after at every 3 years.

d. Governance

- Computer Centre is responsible to devise a mechanism for management of registration and access policy for all users
- The University will make every effort to ensure a fair implementation of this policy in order to meet the objectives. The University's governance structure is responsible for managing the operational aspects of information technology resources. The respective Heads of the Institutions shall be responsible for compliance with all University policies.
- The university will adhere to its e-governance policy for the effective use of IT assets and shall make sufficient budgetary provision every year.
- The University Technology Committee shall strive to standardize the terms & conditions as well as the process for the procurement of IT equipment and software in line with the IT Policy or guidelines of the state government as well as accounting and auditing provisions.
- It is desirable that all Faculties and Departments plan their IT requirements in advance and provide for the same in their budgets. The specifications and configuration submitted for procurement must be consistent with the intended usage and should be derived in consultation with members of the university technology committee

- The university Technology Committee will coordinate various activities related to compliance with the IT policy in collaboration with the Institute IT Administrators.
- The individual users are solely responsible for the activities they perform on Institute/University servers

VI. Violation of Policy:

Any violation of the basic objectives and areas mentioned under the IT Policy of the University shall be considered as a violation and as a misconduct under University Rules.

VII. Implementation of Policy:

For implementation of this policy, the University will decide necessary rules from time to time.

VIII. Review and Monitoring:

The Policy document needs to be reviewed at least once in a year and updated if required, so as to meet the pace of the advancements in the IT related development in the industry.

Review of this policy document shall be done by a committee chaired by Hon'ble Vice Chancellor of the University. The other members of the committee shall comprise of the Technology Committee Members, and other members as nominated by the Chair.