Information Technology IT Policy

Information Technology IT Policy is relevant to all students, faculty members, employees and all the users who utilize the IT infrastructure provided by the institution, SKC. This infrastructure includes all part of the Institution's network such as lab equipment, desktops/laptops, communication nodes, IT/ICT facilities. The policy governs how users access, transmit, or store institutional or personal information within this network.

1. Policy Statement

IT/ICT resources offered by the Institution are intended solely for educational, research, and learning purposes for the users. Users are responsible for the proper utilization and protection of these institutional IT assets, as well as for respecting the rights of others. This policy serves as a guide for the secure and lawful use of the available IT resources and Infrastructure.

2. Guidelines for IT Utilization and Restrictions

- Each user at the Institution is provided with a unique username and password to access the internet. It is expected that users will utilize these resources effectively. This includes internet access, wireless resources and various official websites such as the Institute's main site, conference sites, journal portals, the Institute's Moodle, and course websites. Users also have access to the Institute Management Systems (IMS), the Swayam/NPTEL portal, and facilities that allow remote login to the Institute's systems. In addition, e-Library resources are available for academic and research purposes. Users are encouraged to make use of these comprehensive digital resources.
- The Institution places a strong emphasis on the need for users to adhere to its policies and legal obligations, which include licenses and contracts.
- The Institution is committed to organize awareness programmes aimed at familiarizing users with the optimal utilization of IT resources.
- Prohibited Use - Users are strictly forbidden from sending, viewing, or downloading any content that is fraudulent, harassing, obscene, threatening, or otherwise in violation of applicable laws or Institute policies. The Institution's Sophos firewall is in place to enforce these restrictions and ensure a safe and respectful digital environment for all users.
- Social Media - Users are required to adhere to the Institution's guidelines regarding the use of social media platforms. This includes social networking sites, mailing lists, newsrooms, chat rooms, and blogs.
- Commercial Use - The utilization of the Institution's IT resources is strictly prohibited to any commercial or promotional activities, including advertisements, solicitations or any other form of message dissemination.
- Copyrights and Licenses - Users are obligated to adhere to copyright laws and honour the licenses of copyrighted materials. It should be noted that engaging in illegal file-sharing activities using the Institution's information resources constitutes a breach of this policy.

3. **Security and Integrity**
   - **Personal Use** - The IT resources provided by the Institution should not be employed in activities of violating the basic functionality and mission of the Institution except in a purely incidental manner.
   - **Unauthorized Access** - Users are required to refrain from unauthorized access to information as a measure to uphold the security and integrity of the Network and Computer systems.
   - **System Administrator Access** - The authorized system administrator may access the information resources only for legitimate purposes aligned with their role and responsibilities.
   - **Firewall** – The Institution utilizes a Sophos Firewall as a robust security measure to safeguard against potential threats originating from web pages and commercial websites. This ensures the protection of the Institution's users from risks. The firewall plays a crucial role in managing and maintaining the secure flow of traffic, both from the internet and within the Institution's intranet and it ensures more secure and control network environment within the campus.
   - **Anti-virus and security updates** - Regular updates to the anti-virus policy and security measures are a critical aspect of the Institution's cyber security strategy. The Institution places a high priority on the regular updating of its anti-virus policy and security updates. This is crucial for the protection of its computing resources.
4. **IT Asset Management:**
   - **Asset Management**: The Institution is dedicated to implement robust business processes for the efficient management of its hardware and software assets. These processes aim to enhance the utilization of IT resources within the Institution. They include comprehensive procedures for the acquisition, deployment, maintenance, utilization, energy auditing, and disposal of software and hardware applications.
   - **Copying and Distribution**: The Institution is steadfast in its commitment to respect the rights of proprietary and licensed software.
   - **Risks**: The Institution prioritizes the effective management of risks associated with the utilization of IT resources. This involves the establishment of standard procedures for the identification, reduction, and ongoing monitoring of risk impacts, supported by protective and corrective actions. The Institution ensures the implementation of procedures for prompt data backup, replication and restoration policies, power backups, audit policies and provides alternate internet connectivity to guarantee uninterrupted internet access.
   - **Open Source Advocacy**: The Institution is committed to foster the adoption and efficient application of open source software, striving to be a beacon in the realm of open source technology.

5. IT Hardware Installation Policy

- Installation of software and hardware is done in all the computers of the Institution by system admin and the technical team.
- SKC's IT team ensures safety in installation of hardware.

6. Warranty & Annual Maintenance Contract

- Computers procured by any Section, Department, or Project should ideally come with a 3-year on-site comprehensive warranty. Following the warranty period, the system administration and technical team will be responsible for maintaining the systems.
- Annual Maintenance Contract includes OS re-installation and checking virus related problems.

7. Network Cable Connection

- When connecting the computer to the network, ensure that the network cable is positioned away from any electrical or electronic equipment, as they can interfere with network communication. Additionally, avoid sharing the power supply with other electrical or electronic devices connected to the computer and its peripherals.

8. Noncompliance

- SKC faculty, staff and students should not fail to adhere to the computer hardware installation policy. Otherwise it may expose them to network-related issues and lead them to damaged or lost files which results productivity loss. Non-compliant computers at the individual level can have far-reaching adverse effects on individuals, groups, departments, or even the entire Institution. It is crucial to promptly bring all computers into compliance once any deviations are identified. Noncompliance with the above guidelines may result in punitive actions.

9. Software Installation

- The installation of Institutional software on all computers at SKC is carried out by the system administrators and the technical team.
- The system administrator ensures the smooth functioning of Institution's IT infrastructure. The system admin collaborates with various stakeholders (faculty, staff, students) to understand the Institution's requirements and identify specific needs, such as academic software for classrooms, administrative tools for staff or other applications. The system admin evaluates software and hardware and checks requirements, network compatibility and security considerations. Regular maintenance, updates, and patches are part of their responsibilities. When issues arise, the system admin provide technical support to users, addressing queries and resolving issues promptly.

10. Operating System and its Updating

- The college system administrator and technical team play a pivotal role in selecting the most suitable operating system for the Institution. The system admin and team assess the specific requirements of the college. They evaluate the compatibility of

the operating system with existing hardware and software applications used by faculty, staff, and students. The system admin considers long-term support and vendor reliability.

- Develop standardized OS images, equipped with pre-set configurations and software, to facilitate swift deployment on both new and existing systems.

11. Backups of Data

- Individual users should perform regular backups of their vital data. It is essential to take preventive measures to safeguard valuable files and documents form Virus infections. Regular data backups are the best defence against such Virus infections.
- In SKC regular backup process established, to ensure all college data is securely stored on the dedicated file server

12. Violation of Policy

In accordance with the IT Policy of the Institution, any breach of the fundamental objectives and areas outlined therein will be regarded as a violation and misconduct. Appropriate penalties or punitive actions may be taken as necessary. It is crucial for all members of the Institution to adhere to these guidelines to maintain a secure and ethical computing environment.

13. Implementation of Policy

In the context of implementing the IT policy, the Institution will periodically review and establish necessary rules to ensure compliance and effective management. These rules may evolve over time to address emerging challenges and technological advancements. It is essential to stay informed about any updates or changes to the policy to maintain a secure and efficient computing environment.

Signature of the Secretary

Secretary
SRI KALISWARI COLLEGE,
SIVAKASI.

Signature of the Principal

Principal
SRI KALISWARI COLLEGE
(Autonomous)
SIVAKASI - 626 130