Information Technology Policies, 2020

1. Introduction

Stella Maris College recognises the critical nature of Information Technology (IT) services in higher education in the 21st century, given the exponential growth of the use of digital tools in every area of functioning. Students and faculty are increasingly dependent on digital formats for sharing information both within and outside the institution. Stella Maris College recognises the importance of facilitating IT use, protecting data and updating technologies to keep abreast of global developments.

1.1 Background and Purpose

The Information Technology (IT) policies of Stella Maris College exist to enable, maintain and secure appropriate and permissible use of the College's information technology infrastructure. The policies reflect the institutions vision and mission objectives while articulating the strategy and directions for the operation, use and upgrading and updating of information technology. This policy sets forth responsible and acceptable use of IT resources on campus in order to advance the institutions vision and mission. These resources are provided for teaching and learning purposes, research, and administrative functioning of the institution. They are accessible to all students, faculty, staff, administrators, authorised guests, and others who have permission of the Head of the institution.

2. Definition of Information Technology Resources

The definition of Information Technology Resources (ITR) for the purposes of this Policy include, but are not limited to the transmission cables on campus, servers, cloud storage, wireless networks, internet connections, all software under license for educational purposes, institutional PCs and computer/digital accessories in departments, offices, lecture halls, and audio-visual rooms, computers in laboratories and browsing centres, projectors, laptops, wired networks, LANs, internet connectivity, intranet, College website, institutional email accounts, printers, copying machines, media room, data in digital format, and digital technology deployed in any other dedicated space on campus.

The use of personal digital devices used on campus (laptops, iPads, iPhones, Android phones or any other device) shall conform to the appropriate and relevant regulations given in this policy.

Violations of any clause leading to compromised cyber security on campus will result in severe sanctions, including banning of the use of personal digital devices on campus for that individual.

2.1. Scope

This Policy applies to all members of the Stella Maris Community, alumnae, retired staff and faculty, authorised guests, consultants, and any other person who has the express permission of the Head of the institution to use SMC IT resources on campus. All those who have access to institutional IT are responsible for ethical use of all data/devices/technology available, and their privacy is ensured.

3. Policy Statements

3.1. Stella Maris College IT resources are provided to authorised users only for the advancement of the mission and vision of the institution and to enable and support the functioning and operations of the different constituents of the institution.

3.2. Authorised users shall take care to ensure the safety, confidentiality and security of all SMC IT resources.

3.3. Authorised users shall respect the Intellectual Property Rights of other members of the SMC community.

3.4. Authorised users shall use IT resources in accordance with the SMC IT Policy, Online/Remote Teaching Policy, and other Policy directives of the institution.

4. Code of Conduct

The Policy integrates the Code of Academic Integrity which applies to all students and research scholars, administration and everyone who makes use of technology on campus. It prescribes not only adherence to integrity and ethical use of resources both online and offline, but also to use of the institution's digital resources. This includes computer and network violations such as hacking, introducing a worm or virus, illegally obtaining computer passwords and altering data, unauthorised access to data, computers and networks,

using the institutions ITR for commercial/personal purposes, infringement of copyright, harassment of another user, disclosing sensitive and confidential data/information to unauthorised persons, and physical damage to ITR.

Violations of the Code of Conduct by students shall be handled by the Deans of Student Affairs, faculty by the Vice-Principals and administrative staff by the Secretary of the College in consultation with the Principal. In all sanctions and rulings, the decision of the Principal shall be final. The right to deny access to ITR on campus rests with the Principal and her decision shall be final.

5. Wi-Fi

Wireless networking is an important aspect of technology deployment on campus since it offers many benefits that support the institutional mission. It is one of the objectives of this policy to ensure that wireless connections are centrally controlled and deployed to provide optimal levels of service and ensure maximum security. The institution prohibits the installation of non-standard or misconfigured wireless access points. The purchase and installation of wireless equipment is centralised to ensure that inappropriate devices are not installed and used on the institutions' networks. All resolution of hardware, software, or network issues shall be the responsibility of the respective IT Teams. Any Access Point which is connected to the institutions network infrastructure is the responsibility of the relevant team from the IT Unit. Only devices authenticated by the IT teams may access network resources.

6. Cyber Security

The institution reserves the right to use two levels of security: Site Blocking with Sonic Wall and website blocking with Fort iGATE firewall.

PRINCIPAL
STELLA MARIS COLLEGE
(AUTONOMOUS)
17, CATHEDRAL ROAD,
CHENNAI - 600 086.