St Joseph College of Communication
Media Village, Changanassery
Affiliated to Mahatma Gandhi University, Kottayam, Kerala
Vision: Transforming Media for a Wholesome World

Founded in 2004

Information Technology Policy

Responsible Executive	**IT Head, St Joseph College of Communication**
Responsible Office	**IT Division, St Joseph College of Communication**
Date Issued	**November 2020**
Date Last Revised	**November 2023**
Code	**SJCC/INSP/23/23**

1. Statement of Policy

IT Policy is being documented for fair and transparent use of various IT resources on the Campus for Students, faculty, Staff, Management and visiting Guests, Research Scholars and other entities whatsoever upon the sanction of the head of the institution. St Joseph College of Communication is equipped with a wide array of IT infrastructure and resources serving 3 buildings across the campus. SJCC IT Division shall be solely responsible for the functioning of campus Intranet and Internet services, inter alia- Firewall security, email, website, LMS and other services. St Joseph College of Communication has subscribed to a high-speed dedicated leased line internet facility with a bandwidth of 100+50 Mbps. To secure the network, our IT Division has been taking appropriate steps based on the drafted IT Policy by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway. The faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the information technology infrastructure of the college, must comply with the guidelines.

Certain violations of IT policy laid down by the college by any member may even result in disciplinary action against the offender by the college authorities. If the matter involves illegal action, law enforcement agencies may become involved.

For smooth implementation of IT Policy, the IT Division needs the latest information from the different Administrative Department for providing network and other IT facilities to the new members of the college and for withdrawal of these facilities from those who are leaving the institution, and also for keeping the St Joseph College of Communication web site up-to-date in respect of its contents. The information that is required could be broadly following:

- Information about New Appointments.
- Information about Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Information on Important Events/ Achievements.
- Information on different Rules, Procedures, and Facilities.

2. Objectives

The objectives of the IT policy are as follows:

- To administer, manage, and regulate IT-related operations on the campus regularly and modify the procedure to reflect changing technology, changing requirements of the IT user community, and operating procedures.
- To facilitate users about the steps that are taken for managing the network.
- To provide all required IT resources as per the academic programs laid down by UGC and apex bodies. Also, introduce new IT technologies which will benefit the students, research scholars and staff.
- To effectively have an annual plan of introducing new technologies in line with the Academia.
- Create provision for priority up-gradation of the IT-related products and IT-enabled services on the campus.

- Create Provision for Annual Maintenance expenses to ensure maximum uptime of the products.

- To ensure that the products are updated and catered 24x7 on the campus or as per the policies laid down by the College Management.

3. Scope of IT Policy

3.1 IT policy is affected by the Stakeholders on campus or off campus including

- Students: UG, PG

- Faculty

- Administrative and Supporting Staff

- Guests

3.2 The user must know the IT policy of the college and follow the guidelines to make proper use of the campus IT infrastructure and information resources.

The following Resources also come under the purview of the IT policy

- Network Devices wired/ wireless, CCTVs

- Internet Access

- Official Websites, web applications

- Official Email services

- Learning Management Solution (Linways)

- Meeting Platforms (Zoom, G meet, MS Teams, Skype)

- Data Storage (One Drive with 1 TB per user, Google Workspace with 1 TB per user)

- Desktop/Laptops/ server computing facility

- Documentation facility (Printers/Scanners)

- Display devices (Digital Board/ Digital Projectors)

- Social Media Platforms (Facebook, Instagram, Twitter, YouTube)

4. Role and Responsibilities

IT Division will be responsible for solving the hardware-related problems or OS or any other application software that was legally purchased by the college and installed by the IT

Division and all network-related problems or services related to the network like

4.1 Campus Network Management

- The campus network and its active components are administered, maintained and controlled by the IT Division

- IT Division operates the campus network backbone such that service levels are maintained as required by the Institute Departments, and hostels served by the campus network backbone within the constraints of operational best practices.

4.2 Maintenance of Computer Hardware & Peripherals

IT Division is responsible for the maintenance of the college-owned computer systems and peripherals that are under warranty or out of warranty

4.3 Installation of New IT Equipment and Resources

IT Division identifies the requirement of new IT equipment and resources installation in various offices/departments and finalises the specification of the IT equipment analysing the quotations submitted for the same and makes recommendations regarding

4.4 Troubleshooting Complaints

IT Division may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems. The designated person in the IT Division (Network Administrator) receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems (which are in warranty) to resolve the problem within a reasonable time limit. For out-of-warranty computer systems, problems are resolved at the IT Division. IT Division may receive complaints from departments/users; if any of the network-related problems are noticed by them such complaints should be made by email/phone. IT Division may receive complaints from the users if any of the users are not able to access the network due to a network-related problem at the user end. Such complaints may be generally through phone calls. The designated person in the IT Division receives complaints from the users and coordinates with the user/service engineers of the network hardware or with the internal technical team to resolve the problem within a reasonable time limit.

4.5 Physical Demarcation of Campus Buildings' Network

- Physical connectivity of campus buildings already connected to the campus network is the responsibility of the IT Division

- Physical demarcation of newly constructed buildings to the "campus network" is the responsibility of the IT Division. It essentially means that exactly at which location the fibre optic-based network terminates in the buildings will be decided by the IT Division. How the building is to be connected to the campus network (whether the type of connectivity should be fibre optic, wireless or any other media) is also the responsibility of the IT Division.

- IT Division will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.

- It is not the policy of the college to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the College Internet links.

4.6 Wireless Local Area Networks

- Where access through Fiber Optic cables is not feasible, in such locations IT Division considers providing network connection through wireless connectivity.

- IT Division is authorized to restrict network access to the offices, departments, or hostels through wireless local area networks either via authentication or MAC/IP address restrictions.

4.7 Network Expansion

Major network expansion is also the responsibility of the IT Division. Every 3 to 5 years, the IT Division reviews the existing networking facilities and the need for possible expansion.

4.8 Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

4.9 Global Naming & IP Addressing

IT Division is responsible for providing a consistent forum for the allocation of campus network services such as IP addressing and domain name services. IT Division monitors the network to ensure that such services are used properly.

4.10 Providing Net Access IDs, email Accounts, LMS username and Office 365 Login

IT Division provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the institute upon receiving the requests from the individuals on prescribed proforma.

4.11 Video Surveillance

IT division is responsible for the maintenance of the Video Surveillance mechanism installed on the campus. The system comprises around 400 fixed-position cameras; Monitors; digital video recorders; Storage; and Public information signs.

4.12 Meeting Platform Management

IT Division is responsible for managing the Online Meeting platforms (Zoom, G Meet, MS Teams, and Skype) of the college. IT division will issue meeting links for official programmes of department/ clubs/ and common programs of the college based on formal requests from the person concerned coordinating the programme. Backup of the recorded video of the programme will be available for 24 hours.

4.13 Website Management

IT division is solely responsible for the management of the College website. Upgradation and maintenance of the college website will be done from time to time. Home Page management, Notice and Announcement shall be updated internally by the IT division and further upgradation in the website will be done with the support of external agencies managing the website.

4.14 Social Media Page Management

IT division is responsible for managing the official social media pages (Facebook, Instagram LinkedIn and Twitter) of SJCC. News and updates about various programmes organized by the college/departments/ clubs and associations will be published through social media pages subject to approval from the head of the institution.

4.15 Disconnect Authorization

IT Division will be constrained to disconnect any Department, office, or hostel from the campus network backbone whose traffic violates practices outlined in this policy or any network-related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Department, office, hostel machine or network, the IT Division endeavours to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Department or division is disconnected, the IT Division provides the conditions that must be met to be reconnected.

5. Policy Area

5.1 Software Installation

Any computer system purchased made by the individual/departments/office should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, the College does not allow any pirated/unauthorized software installation on the college-owned computers and the computers connected to the campus network. In case of any such instances, the College will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/office

5.2 Email Account Use

To increase the efficient distribution of critical information to all faculties, staff and students, and the administrators, it is recommended to utilize the College e-mail (G suit) services, for formal communication and academic & other official purposes. Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the College to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general messages, notices, official announcements, etc. To receive these notices, the e-mail address must be kept active by using it regularly. Staff, faculty and students may use the email facility by logging on to https://gmail.com with their User ID and password. To obtain the college email account, the user may contact the SJCC IT division for

an email account by applying a prescribed proforma.   Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes only.

- Using the facility for illegal/commercial purposes is a direct violation of the College IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

- Users should not open any mail or attachments that are from unknown and suspicious sources. Even if it is from a known source, and if it contains any attachment that is suspicious or looks dubious, the user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have the potential to damage the valuable information on your computer.

- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

- Impersonating the email accounts of others will be taken as a serious offence under the institute's IT security policy.

- A staff email account will be deactivated as and when he/she retires, resigns or is terminated

- A student's email account will be deactivated as and when a student completes his regular period of study in the college.

- It is ultimately each individual's responsibility to keep their e-mail account free from violations of the institute's email usage policy.

The above laid down policies are broadly applicable even to the email services that are provided by other email providers., as long as they are being used from the campus

network, or by using the resources provided by the college to the individual for official use even from outside.
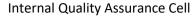
5.3 Net Access ID Management

Any type of user can connect to the College network using a legitimate user account (Net Access / Captive Portal ID) for verification of affiliation with the college. The user account will be provided by the IT division, upon filling up the prescribed application form and submitting it to the IT division. Once a user account is allocated for accessing the campus computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the college authorities for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access ID and for email account ID to prevent unauthorized use of their user account by others.

5.4 LMS User Management

All users (faculty, staff, and students) can access the Linways portal (LMS) of the college. The user credentials of faculty members will be provided by the IT division at the time of appointment of new staff in any of the departments upon filling up the prescribed application form and submitting it to the IT division. User credentials of students will be provided by the IT division after completing the admission procedure.

5.5 Video Surveillance

Around 400 CCTV cameras are located at strategic points on the campus, principally at the entrance and exit points of sites and buildings. Video surveillance data will be stored in the server with a one-month backup period. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

A video surveillance system has been installed by the college with the primary purpose of reducing the threat of crime generally, protecting college premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individual's privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent

- Assist in the prevention and detection of crime

- Facilitate the identification, apprehension and prosecution of offenders concerning crime and public order

- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

It is recognized that members of the institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instance to the IT wing. CCTV footage provided by the College upon receiving the requests from the individuals on prescribed proforma.

5.6 Web Site Management

The IT department ensures the updation of the happenings of the college daily. The domain shall be renewed as per the contract.

5.7 Hardware Installation

IT Division is responsible for the maintenance of the college-owned computer systems and peripherals that are under warranty or out of warranty*.* Complaints regarding hardware can be made at the Grievance redressal cell and timely action will be taken by the IT wing.

5.8 Social Media Page Management

The IT department ensures the updation of the happenings of the college daily on social media platforms.

6. Approval & Review Details

Approval Authority:

Executive Director, St Joseph College of Communication

Officer In-charge:

IT Head, St Joseph College of Communication

Approved on: November 2023

Next Review Date: November 2024

7.   Feedback:

Stakeholders may provide feedback about this document by e-mailing IQAC.