Information Technology Policy

Volume	II
Responsible Executive	IT Head, St. Berchmans College
Responsible Office	IT Division, St. Berchmans College
Date Issued	November 2020
Date Last Revised	November 2022

1. Statement of Policy

IT Policy is being documented for fair and transparent use of various IT resources in the Campus for Students, faculty, Staff, Management and visiting Guests and Research Scholars and other entities whatsoever upon the sanction of the head of the institution. St Berchmans College equipped with wide array of IT infrastructure and resources serving 21 buildings across the campus. Berchmans IT Division shall be solely responsible for the functioning of campus Intranet and Internet services, inter alia- Firewall security, DHCP, email, web site, LMS and other services. SB College has subscribed to high speed dedicated leased line internet facility with bandwidth of 250 Mbps. In order to securing the network, Berchmans 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, IT Division needs 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 institute, and also for keeping the SB College web site up-to-date in respect of its contents. The information that is required could be broadly of the following nature:

- 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, regulate IT related operations in the campus on a regular basis 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 is 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 and 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 in 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 in the campus or as per the policies lay 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, M Phil and Research

- Faculty (Aided/ Self Financing/ Temporary/Contractual)

- Administrative Staff (Aided /Management/)

- Guests

3.2 It is the duty of the user to 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 comes under the purview of the IT policy

- Network Devices wired/ wireless

- 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, You Tube)

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 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 maintenance of the college-owned computer systems and peripherals that are under warranty or out of the warranty

4.3 Installation of New IT equipment and Resources

IT Division identifies the requirement of new IT equipment and resources installation in various office/department and finalise the specification of the IT equipment and analysing the quotations submitted for the same and make recommendations regarding

4.4 Trouble shooting Complaints

IT Division may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them is having any problems. The designated person in 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 resolved at IT Division. IT Division may receive complaints from department/users; if any of the networks 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 is 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 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 IT Division

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

4

- 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 Fibber 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 IT Division. Every 3 to 5 years, 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 the ends, at which time they should be destroyed.

4.9 Global Naming & IP Addressing

IT Division is responsible to provide 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 ID's, 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 Video Surveillance mechanism installed in the campus. The system comprises around 75 fixed position cameras; Monitors; digital video recorders; Storage; 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 link for official programmes of department/ clubs/ and common programs of the college based on formal request from the person concerned coordinating the programme. Back up 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 web site. 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 up gradation in the website will be done with the support of external agency managing the website.

4.14 Social Media Page Management

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

4.15 Disconnect Authorization

IT Division will be constrained to disconnect any Department or office, hostel from the campus network backbone whose traffic violates practices set forth 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, or office, hostel machine or network, 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, 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, College does not allow any pirated/unauthorized software installation on the

St Berchmans College
AUTONOMOUS | College with Potential for Excellence | Reaccredited by NAAC with A Grade
Affiliated to Mahatma Gandhi University, Kottayam, Kerala
Changanassery, Kottayam, Kerala, India-686101

Internal Quality Assurance Cell

college-owned computers and the computers connected to the campus network. In case of any such instances, 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

In an effort 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 for 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 and official announcements, etc. To receive these notices, it is essential that the e-mail address 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. For obtaining the college email account, user may contact Berchmans IT division for email account by submitting an application in 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, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, 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 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 email account of others will be taken as a serious offence under the institute IT security policy.

- A staff email account will be deactivated as and when he/she retires or resign or terminated the from employee roll of the college

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

- It is ultimately each individual's responsibility to keep their e-mail account free from violations of 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 the purposes of verification of affiliation with the college. The user account will be provided by IT division, upon filling up the prescribed application form and submitting it to 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 un-authorized use of their user account by others.

St Berchmans College
AUTONOMOUS
Affiliated to Mahatma Gandhi University, Kottayam, Kerala
Changanassery, Kottayam, Kerala, India-686101

Internal Quality Assurance Cell

5.4 Office 365 Login Management

All faculty members can use the office 365 purchased by the college IT division. The user account will be provided by IT division, upon filling up the prescribed application form and submitting it to IT division. By using the office 365 access credentials faculty can access 30 apps included in office 365 including Prezi, MS teams, share points one drive etc.

5.5 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 IT division at the time of appointment of a new staff in any of the department upon filling up the prescribed application form and submitting it to the IT division. User credentials of students will be provided IT division after completing the admission procedure.

5.6 Video Surveillance

Around 75 CCTV cameras are located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. Video surveillance data will be stored in the server with one month back up 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.

Video surveillance system has been installed by 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 individuals' 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 in relation to 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 instant to the Computer Center. CCTV footage provided by the College upon receiving the requests from the individuals on prescribed proforma.

5.7 Web Site Management

5.8 Hardware Installation

5.9 Social Media Page Management

6. Approval & Review Details

Approval Authority:

Manager, St. Berchmans College, Changanacherry

Officer In charge:

IT Head, St. Berchmans College

Approved on: November 2022

Next Review Date: November 2024

7. Feedback:

Stake holders may provide feedback about this document by e-mailing to IQAC.