IT Policy of Carmel College (Autonomous) aims to ensure the responsible and beneficial use of IT infrastructure for the entire college community, including students, teachers, supporting staff, and the public.

Scope: This policy is applicable to the principal, teaching and non-teaching staff, students, as well as the public who utilize Carmel College's IT infrastructure. The users are solely responsible for the activities they perform on institute/ College servers with their username/passwords" pairs and IP address assigned to them. 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 IT team plays a critical role in supporting the academic mission and administrative functions of the college by ensuring the availability, reliability, and security of IT resources and services. IT Team keeps a record of the hardwares and software licenses procured, distribution list, serial numbers, receipts and invoices, Software licensing terms along with the end date of agreement.

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)
- Desktop/Laptops/ server computing facility
- Documentation facility (Printers/Scanners)
- Display devices (Digital Board/ Digital Projectors)

Infrastructure Planning and Upgrades: Planning and implementing upgrades to the college's IT infrastructure to keep pace with technological advancements and accommodate the growing needs of the institution. This may involve hardware upgrades, software updates, and expansion of network capabilities.

Procurement of IT Resources: All requests for purchases of IT resources need to be pre-approved by the Head of the Department and sent to IT team with the approval of Principal. Acquisition of items related to government projects and aids must comply with Kerala Government regulations. The use of unauthorized software on Carmel College computers is strictly prohibited.

Hardware and Software Support: Providing technical support for computers, printers, scanners, projectors, and other hardware devices used in classrooms, labs, libraries, and administrative offices. Additionally, installing, updating, and troubleshooting software applications used for academic and administrative purposes.

Network Management: Maintaining and managing the college's computer networks, including wired and wireless connections, routers, switches, and firewalls. This ensures reliable internet access and connectivity for students, faculty, and staff.

Data Management: Managing the college's data storage systems, including servers, databases, and cloud services, to ensure data availability, integrity, and confidentiality. This may involve data backup and recovery procedures, data archiving, and compliance with data protection regulations.

Responsible Utilization of IT Resources: The utilization of Carmel College's IT resources is confined to academic pursuits and occasional personal usage. Personal usage should not hinder college operations or result in supplementary expenses. Installation of software directly onto institution IT assets is prohibited for all members. Users are expected to abstain from unauthorized information access to ensure the secure usage of Network and Computers. The authorized system administrator may access information resources for valid purposes.

User Support and Training: Providing technical assistance and training to students, faculty, and staff on using IT resources effectively and securely. This may include conducting workshops, creating user guides and tutorials, and responding to helpdesk inquiries.

Operating Systems: Users are accountable for maintaining regular updates to their computer operating systems. Any concerns regarding updates should be directed to the IT Coordinator. Carmel College advocates for the utilization of open-source software, such as Linux and LibreOffice.

E-Learning Support: Supporting the use of technology for online learning initiatives, including learning management systems (LMS), virtual classrooms, video conferencing tools, and educational software applications. This may involve assisting faculty in developing online course materials and providing technical support for students participating in online courses.

Learning Management System (Linways): Every teacher and student is provided with a unique login for Linways ERP, and sharing these credentials is strictly prohibited. Users bear sole responsibility for any misuse of their accounts.

Institutional Email: It is encouraged for faculty and students to utilize the college-provided institutional email accounts for official correspondence. These email accounts should primarily serve academic purposes and must not be used for any illicit activities.

College Website: The college website is managed by the Website Coordinator and IT Team. Prior approval from the Principal is required for any updates or announcements, which should then be directed to the Website Coordinator. Additionally, Carmel College supports the creation of personal and departmental web pages.

Video Surveillance: Surveillance cameras are strategically placed throughout the campus, monitoring entrances, exits, exam halls, and hostels. These cameras are engineered to preserve privacy, and access to recorded footage is restricted to the Principal and authorized personnel designated by the Principal, as necessary.

Cybersecurity: Implementing and managing security measures to protect the college's network, systems, and data from cyber threats such as malware, viruses, hacking attempts, and data breaches. This includes installing and updating antivirus software, firewalls, intrusion detection systems, and conducting regular security audits. The use of external storage devices such as pen drives and CDs is discouraged except in special circumstances.