ST PHILOMENA COLLEGE

Affiliated to Mangalore University Re-Accredited by NAAC at 'A' Grade

MAI DE DEUS EDUCATIONAL INSTITUTIONS

Managed by the Catholic Board of Education, Mangalore

Philonagar, Darbe, Puttur - 574202, D.K., Karnataka | 08251 230340

www.spcputtur.ac.in | info@spcputtur.ac.in | Office : 08251-230340 | Principal : 08251-236460 | 9901380340

INFORMATION TECHNOLOGY RESOURCE USE POLICY

ST PHILOMENA COLLEGE
Date:..........
No:..........
IQAC

1. INTRODUCTION

This document formalises the policy for academics, staff, students, and anyone else who has been authorised access to information technology resources St Philomena College("Users"). This policy and the college's Code of Conduct govern non-college computers, including personal computers and other electronic devices, accessing and using the college's electronic information and information systems. This policy covers the use of information systems acquired or created with college funds, including grant funds from contracts between the College and external funding sources (public and private).

Computers, local and wide area networks, printers, various peripherals, software systems, data, electronic mail, and the Internet are just a few examples of information technology resources. As stated in this document, access to college computer systems and networks comes with it some responsibilities and obligations. Users are permitted to utilise information technology resources in accordance with college regulations as well as local, state, and union laws. Acceptable use is always ethical, indicates academic integrity, and shows restraint in the use of shared resources. It displays a commitment to intellectual property, data ownership, system security, and individual privacy rights. Acceptance of the provisions of this policy, as well as any other applicable College policies, rules, and procedures is required while using information technology resources.

2. USER RESPONSIBILITY

Members of the St Philomena College community have access to and use of technology resources in order to support educational, research, and service purposes. E-mail, computer hardware and software, Internet access, and the campus computer network are examples of such resources of the college. St Philomena College owns all technology resources, as well as their components and peripheral parts. It is the obligation of all users to make efficient, ethical, and legal use of such resources. Authorized users only have access to certain resources, and they can only use them for approved purposes. Lobbying or political campaigns should not be conducted using college IT resources. Furthermore, such resources should not be used for private business or commercial purposes, unless such activities are specifically approved by applicable college policies.

Employees are allowed to use IT facilities for personal reasons, just as they are allowed to use the telephone. Personal use is permitted as long as it does not interfere with job performance, consume significant time or resources, interfere with others' activities, or violate this policy in any other way.

Students who are given access to the college computer facilities and the campus-wide communication network are responsible for its proper use. In their use of computers and networks, the college expects students to be cautious, honest, responsible, and courteous. Students who use wide-area networks (such as the Internet) to communicate with others or connect to computers at other institutions must follow both the rules for remote systems and networks and the rules for college systems.

Anyone who uses the information technology resources of the college is responsible for reading, understanding, and adhering to this policy. Users must also follow all other applicable College policies and procedures, as well as all applicable state and union laws. Any questions regarding this policy should be directed to the principal.

3. ACCEPTABLE USE

The information technology resources and services of the college may be used only for academic, educational, or professional purposes which are directly related to official College business and in support of the Mission of the college. They are not provided for personal use. The use of information technology resources is integral to enhancing productivity in the daily office routine and enabling faculty, staff, and students to make use of research and educational opportunities. The College expects users to access and use the electronic information and information systems in a manner that:

- Does not compromise the confidentiality, integrity, or availability of those assets; and
- Reflects the standard of the college as defined in the Code of Conduct and its body of policies, and in accordance with all applicable federal, state, and local laws governing the use of computers and the Internet.

These obligations apply regardless of where access and use originate: college office, classroom, public space, lab, at home, or elsewhere outside the College.
The rules stated in this policy also govern the use of information assets provided by the State of Massachusetts, other state and federal agencies, and other entities that have contracted with college to provide services to their constituents and/or clients.

Schools, units, and departments may produce more restrictive policies. Therefore, users should consult with their department if there are any other restrictions in place that supplement this policy. Acceptable information technology uses may include but are not limited to:

- Using classroom and lab computers for class assignments
- Preparing instructional materials
- Publishable research
- Personal computing to improve computer literacy and to learn new software and/or hardware
- Accessing generally available individual and campus information
- Using the technology to support faculty and staff in performing their work
- Authorized and approved use of the information and administrative systems of the college
- Using the Internet to promote collegial and professional interaction, research and productivity
- In making acceptable use of resources, one must:
- Use resources only for college business, for purposes authorized by the College.

ST. PHILOMENA COLLEGE
Date:........
No:................
IQAC

- Use the College website, server and all other related computer equipment and services only for academic, educational, or professional purposes which are directly related to official College business and in support of the mission of the college.
- Be responsible for all activities conducted on one's user ID or that originate from his/her system that result from his/her negligent failure to protect the user ID or to protect against such unauthorized use.
- A user is prohibited from disclosing his / her user ID to anyone for use on the computer network of the college.
- Access only files and data that are your own, that are publicly available, or to which one has authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in the use of shared resources. Examples include not monopolizing systems, overloading networks with excessive data, or wasting computer time or resources, disk space, printer paper, manuals or other resources.

4. UNACCEPTABLE USE

The list of prohibited actions is not intended to be comprehensive. The evolution of technology precludes the College from anticipating all potential means of capturing and transmitting the information. Therefore, users must take care when handling sensitive information.

In making acceptable use of resources, one must not:

- Disclose/Distribute information classified as Confidential or Private, or otherwise considered or treated as privileged or sensitive information, unless they are an authoritative College source for, and an authorized College distributor of, that information and the recipient is authorized to receive that information.
- Share their passwords with other individuals or institutions (regardless if they are affiliated with the college or not) or otherwise leave them unprotected.
- Use another person's user ID or password.
- Use another person's files or data without permission.
- Use third party email services to conduct sensitive College business or to send or receive College information classified as Confidential or Private, or otherwise considered privileged or sensitive information.
- Use computer programs to decode passwords or access control information.
- View, download, store or transmit pornographic materials or obscene materials.
- Circumvent, subvert, or attempt to circumvent or subvert system or network security measures.
- Purposely engage in any activity that might be harmful to system/network or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.

- Make or use illegal copies of copyrighted software, store such copies on College systems, or transmit them over College networks.
- Use the network for purposes which place a heavy load on scarce resources.
- Use College computers or networks to harass any other person. The following shall constitute Computer Harassment: (1) using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (3) using the computer to disrupt or damage the academic research, administrative, or related pursuits of another; (4) using the computer to invade the privacy, academic or otherwise, of another or threatened invasion of privacy of another.
- Waste computer resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- Use the systems or networks of the college for personal gain; for example, by selling access to your user ID or to college systems or networks, or by performing work for profit with college resources in a manner not authorized by the College.
- Use any other College-related systems or networks to transmit any material in violation of national laws or regulations.
- Engage in recreational game playing or online gambling.
- Intercept communications intended for other persons.
- Misrepresent either the College or a person's role at the College.
- Infringe on any intellectual property rights.
- Distribute chain letters.
- Engage in any other activity that does not comply with the General Principles presented above.

This list of unacceptable uses is not intended to be exhaustive.

5. RESTRICTED SERVICES

This list of restricted services is not intended to be comprehensive. The evolution of technology precludes the College from anticipating all potential means of storing, capturing, and transmitting the information. Therefore, when using third-party technology services not explicitly restricted in this policy, users must exercise care to not compromise sensitive College information.
Restricted services include the following:

5.1 SOCIAL MEDIA

The use of all College computer resources for social media activities including, but not limited to, Facebook, YouTube, Twitter, blogs or another form of social media, shall comply with this policy. Use of the College's computer resources by faculty and staff for personal social media activities

ST. PHILOMENA COLLEGE
Date:..........
No:..........
IQAC

is prohibited. Use of the computer resources of the college by students for educational and social activities consistent with the Mission of the college shall comply with this policy. Social media tools cannot be used to communicate or store College information classified as Confidential or Private or otherwise considered privileged or sensitive by College. Social media tools include, but are not limited to: Social networking sites: e.g. Facebook, Google+, Myspace, LinkedIn, Blogs

- Microbloggingng sites: e.g. Twitter, Wikis, Content-sharing services: e.g. YouTube (video) and Flickr (for photos, videos, etc.),
- Online forums
- The College e-mail address cannot be used on social media sites for personal communications or postings.
- Using the College name or e-mail address on social media sites to post information in a manner that may be interpreted as representing an official position of the College, or which may misrepresent the viewpoint of the college. All posting where the user is identified as a member of the College should clearly communicate that, "The views and opinions expressed are strictly those of the author. The contents have not been reviewed or approved by the College.

5.2 CLOUD SERVICES

Cloud Storage Tools – The use of third-party cloud storage services cannot be used to store the College information classified as Confidential or Private or otherwise considered privileged or sensitive by the College. Cloud storage tools include, but are not limited to: iCloud, OneDrive, Office 365.

5.3 DATA SHARING TOOLS

The use of data sharing tools cannot be used to share or store College information classified as Confidential or Private or otherwise considered privileged or sensitive by the college. Data sharing tools include, but are not limited to Microsoft OneDrive, Box.net, Catch, Dropbox, Evernote, Google Docs, Google Drive

5.4 THIRD-PARTY EMAIL SERVICES

Third-party email services cannot be used to communicate or store college information classified as Confidential or Private or otherwise considered privileged or sensitive by the college.

5.5 TEXTING

Users should take care texting other sensitive information, particularly when confirmation of receipt or the identity of the recipient is required for business or legal purposes.

5.6 INTERNET-BASED VIDEO CONFERENCING

Internet-based video conferencing services, such as Skype, are limited to college business use only and must be conducted using college equipment. They are to be used strictly for business

ST. PHILOMENA COLLEGE
Date:..........
No:..........
IQAC

collaboration between members of the College community or outside entities, or for educational purposes. Users must ensure that video communications are done in a setting that limits or restricts the possibility that non-authorized individuals from viewing or listening to sensitive information.

5.7 COPYRIGHT PROTECTION

Computer software is intellectual property. Software publishers and vendors can be very aggressive in protecting their property rights from infringement. These intellectual property rights extend to information published on the Internet, such as text and graphics. Users who buy their own software agree to comply with any and all provisions of the software vendor in the software license agreement. Users are not permitted to copy software made available by the College to any other computer. In instances where a license agreement links a license number to specific computers by serial number, and the hardware is replaced or upgraded, the license agreement but be changed accordingly. All software on all computers on campus must be properly licensed. Information Officer maintains inventories of all computers and all software products installed on each computer. When users have made their own software purchases, it is their responsibility to furnish a license agreement when audited.

5.8 NETWORK SECURITY

Computers at the college are connected to a local area network, which connects them to the Internet. All users should avoid jeopardising the security of the network. Users should never discuss their credentials with others and should tell network administrators right away if they feel their passwords have been hacked. Users who will be away from their computers for a lengthy period of time should either log off the network or use password-protected screen savers.

Text files, executable files, images, word processing documents, spreadsheets, and e-mail communications can all contain viruses, worms, Trojan horses, and other harmful programs. To lessen the likelihood of a successful attack or infection, the College employs technical solutions such as anti-virus, anti-spyware, and anti-SPAM software. To avoid the insertion of harmful code, users should take necessary precautions. Users should not disable virus scanning applications, and instead utilise them to scan files acquired from the Internet or obtained from a shady source, as well as portable media like as compact discs, external hard discs, and USB sticks.

5.9 E-MAIL SYSTEM

The official College e-mail system is Google Workspace. The College provides electronic mail as a supplement to traditional ways of communication and to increase administrative and educational efficiency. The College owns all e-mail accounts and all data transmitted or stored via e-mail services. Broadcast messages to all teachers and staff via the Faculty/Staff e-mail group should only be used for important College announcements that affect the whole College community.

All users should treat e-mail messages as if they were formal written communications, and should use a professional and courteous tone while writing them. It's important to remember that an e-mail message can be saved, copied, printed, or sent to others. A good rule of thumb is to never include anything in an e-mail message that you wouldn't put in a memo, post on a bulletin board, or discuss in a public meeting.

Public Folders are provided as a service for posting general news, events, and other College-related information within the mail system. Those in charge of their content will keep an eye on these folders. Any content that is found to be objectionable will be removed without warning. Public Folders are likewise subject to unique guidelines tailored to the needs of the folder.

5.10 INTERNET USE

The Internet is a valuable resource for many forms of academic activities and promote research. The College is dedicated to supporting safe Internet usage. Internet access should be regarded as a privilege by all users. Many websites collect and keep information on their visitors. Users should be aware of this. When registering for anything online, use caution because you are essentially handing your name, address, and phone number to a stranger. Users must be aware that downloading and installing files from websites, including seemingly innocuous ones, might introduce harmful code onto the College network and PCs. When it comes to downloading software from the Internet, users should exercise utmost caution. Users should be aware of the Internet bandwidth limitations of the college. Users are discouraged from engaging in activities that require large amounts of bandwidth, particularly during peak daytime use periods, in addition to conforming to the College's policy addressing permitted and inappropriate uses. By failing to follow this suggestion, a single user can have a significant negative influence on all College users.

5.11 COLLEGE SOCIAL NETWORK PAGES

The College encourages social network users to connect, but it is not responsible for any comments or postings made by visitors to the pages. The thoughts and policies of the College are also not reflected in the comments. The College is not liable for any damage or loss caused or purported to be caused by or in connection with the publishing of any information on these pages, whether directly or indirectly. The College reserves the right to edit or remove any posts, as well as to block or remove members from the group, but does so without obligation. Commercial or political activities, as well as other non-College-related initiatives, are not permitted. The College has the right to delete any content from pages that is in violation of this or other College policies.

5.12 OFFICIAL WHATSAPP GROUPS

The class teachers create a class-specific WhatsApp group and invite the students to join. The college will implement a social media and data protection policy, which will be followed by all members of the college. WhatApp group promotes collaborative work and content exchange, not only between the school and the students but also among them. It's used for sharing audio lectures, providing PowerPoint presentations, and sending documents like Word, books, and so on. It's also a platform for sharing video material. Also, keep the educational community informed of any institution-related announcements or updates.

All administrators of WhatsApp and similar groups, whether it is a faculty or student will be responsible to:

- Create and manage WhatsApp and similar groups;
- Remove any of the prohibited content;
- Manage membership of the respective WhatsApp group(s);
- Inform members of the policies relating to the management of information and the rules relating to the use of WhatsApp and similar platforms for official purposes;
- Revoke the membership of any member who does not comply with these rules; and
- Delete the WhatsApp or similar group when there is no purpose for the group to exist.

All members, whether it is staff or students will be responsible to:

- Ensure that they comply with the rules for using WhatsApp and similar groups;
- Abide by the instructions from the administrator of the group; and
- To always engage on these platforms in a caring and respectful manner.

6. CONFIDENTIALITY

Data and information stored in the computers of the college and associated systems belong to the College, and its dissemination and use must comply with the policies of the college and procedures. College personnel frequently have access to confidential or proprietary information while performing their responsibilities, such as personal data about identifiable individuals, student record information, or commercial information about companies in contact. Employees may only gain access to confidential data if it is required by their work. Employees may not divulge any confidential information to which they have legal access unless it is necessary by their work. These limits are in addition to any state or union-imposed restrictions or prohibitions on the release of confidential information.

7. YOUR OWN DEVICE

The College understands the benefits for Faculty and Staff to use personal devices for work-related tasks. Information Technology is committed to providing the best user experience to all members of the campus community while maintaining a secure environment. The use of own device when accessing, creating, and managing College data can present issues. The College must ensure the institution remains in control of the data for which it is responsible regardless of the device used to process it.

This policy applies to all members of the College community, which includes, but is not limited to, full and part-time employees, temporary employees, students, third parties, contractors, and consultants (collectively known as "Users") who have access to, support, administer, manage, or maintain the College information technology assets.

All relevant College policies still apply to Faculty and Staff using their own devices.

Access to college-owned data from personally owned devices is permissible from on and off campus when it is required to perform job responsibilities. However, for the security of College-owned data, the following are not permitted:

- Storing a local copy of College-owned data to personal devices
- Accessing College owned data for reasons other than job responsibilities
- Distributing College owned data to non-authorized persons

Faculty or Staff who take advantage of bringing own device must take responsibility for their own device and its use, which includes:

- Familiarize themselves with their device and its security features so they can ensure the safety of College-owned information.
- Make use of relevant security features
- Maintain the integrity of the device concerning Operating System patching and Virus/Malware Definition updates.
- Maintain a support agreement for hardware and software-related issues (IT does not provide support for personal technology devices)
- Monitor the download and installation of malicious software

The College reserves the right to prevent access to a particular device to the campus network or system if the device poses a threat to the integrity of our information technology assets. The College also reserves the right to retrieve and remove College owned data from unapproved devices

8. ENFORCEMENT

On a case-by-case basis, College Management will investigate alleged violations of permissible use standards. Violations of the policy will result in appropriate actions, disciplinary considerations, and/or referral to competent authorities responsible for implementing state and union laws. Users who violate this policy risk losing access to the computer and communications networks, as well as facing additional disciplinary actions of the college. When discipline is imposed, it must be in accordance with the terms of any applicable governing collective bargaining agreement. The College reserves the right to disconnect that user from the network in order to prevent additional possible unlawful behaviour. If college personnel determines that this is required, a reasonable attempt will be made to notify the user prior to the disconnection.

Violations of this IT Policy will be reported to relevant administrators for possible disciplinary action in accordance with college policies and procedures. Any violation of the College's acceptable use principles or guidelines of the college is regarded as a serious offense, and the College reserves the right to copy and review any files or material allegedly relevant to unacceptable use that is stored on college systems. Students and employees who violate policies, may face disciplinary action. Laws may also be used to prosecute offenders.

***

Coordinator
IQAC
St. Philomena College, Puttur

ST. PHILOMENA COLLEGE
Date:..........
No:..............
IQAC

PRINCIPAL
ST PHILOMENA COLLEGE
PHILONAGAR, DARBE, PUTTUR - 574 202