IT POLICY

Introduction

With the convergence of technologies, it has become imperative to take a comprehensive look at all possible information technologies for the quality improvement of teaching learning at St. Mary's PG College Vidisha. The comprehensive choice of IT for holistic development of education can be built only on a sound policy. The initiative to develop an IT Policy of the college is inspired by the tremendous potential of IT for enhancing outreach and improving quality of education. This policy endeavors to provide guidelines to support the stakeholders of St Mary's in optimizing the use of IT resources. Users are currently adhering to all the policies mentioned here.

Objectives

- The objective of the IT Policy is to devise, catalyze, support and sustain IT and IT enabled activities and processes in order to improve access, quality and efficiency in the education system of the college.
- The IT Policy aims at preparing adult learners to participate creatively in the establishment, sustenance and growth of a knowledge society leading to all round socio- economic development of the nation and global competitiveness.

Policy Goals

To achieve the above, the IT Policy in College Education will endeavor to:

- Create an environment to develop a community conversant with technology which can deploy, utilize and benefit from Information technology
- Create an environment of collaboration, cooperation and sharing, conducive to thecreation of a demand for optimal utilization of and optimum returns on the potentials of IT in college education
- Promote development of local and localized quality content and to enable

students and teachers to partner in the development and critical use of shared digital resources

- Promote development of professional networks of teachers, resource persons and colleges to catalyze and support resource sharing, up gradation, and continuing education of teachers; guidance, counseling and academic support to students; and resource sharing, management and networking of college managers and administrators, resulting in improved efficiencies in the teaching-learning process
- Promote research, evaluation and experimentation in IT tools and IT enabled practicesin order to inform, guide and utilize the potentials of IT in college education and also to promote a critical understanding of ICT, its benefits, dangers and limitations
- Motivate and enable wider participation of all sections of society in strengthening the college education process through appropriate utilization of ICT

Importance and role of ICT in an educational institution

Meaning of ICT:

Information and Communication Technology Consists of the hardware, software, networks and media for the collection, storage, processing, transmission and presentation of information (voice, data, text, images and videos) as well as related services.

Information and Communication Technologies are defined as all devices, tools, content, resources, forums, and services, digital and those that can be converted into or delivered through digital forms, which can be deployed for realizing the goals of teaching learning, enhancing access to and reach of resources, building of capacities, as well as management of the educational system.

These will also include processes for digitization, deployment and management of content, development and deployment of platforms and processes for capacity development, and creation of forums for interaction and exchange.

Information and Communication Technologies have enabled the convergence of a wide array of technology based and technology mediated resources for teaching learning. It has therefore become possible to employ ICT as an omnibus support system for education. The potential of ICT to respond to the various challenges posed by the Indian education system are:

- ICT can be beneficially leveraged to disseminate information about and catalyze adaptation, adoption, translation and distribution of sparse educational resources distributed across various media and forms. This will help promote its widespread availability and extensive use.
- There is an urgent need to digitize and make available educational audio and video resources, which exist in different languages, media standards and formats.
- Given the scarcity of print resources as well as web content in Indian languages, ICT can be very gainfully employed for digitizing and disseminating existing print resources like books, documents, handouts, charts and posters, which have been used extensively in the education system, in order to enhance its reach and use.
- ICT can address teacher capacity building, ongoing teacher support and strengthen the

education system's ability to manage and improve efficiencies, which have been difficult to address so far due to the size of the college system and the limited reach of conventional methods of training and support.

- There is an urgent need to develop and deploy a large variety of applications, software tools, media and interactive devices in order to promote creative, aesthetic, analytical and problem solving abilities and sensitivities in students and teachers alike.

The IT Policy of the College is an amalgamation of 5 sub divisions.

I General IT Ethics / Ethos Policy

Purpose

St. Mary's PG College Vidisha is an educational institution, which encourages continuous learning, experimentation, and the development of the adult learner. The College is dedicated to respect privacy and freedom of individuals and expects each individual to act in a responsible, legal, ethical and efficient manner when using information technology systems and resources of thecollege. These systems are designed to encourage high-quality educational, professional & career development and self-discovery & research activities.

The purpose of this policy is to define responsible and ethical use of information technology resources available at St Mary's that guides faculty, student, and staff.

Statement of Policy

St Mary's provides access to information technology resources for faculty, staff, students, and certain other users to support the mission of the college. Every authorized user of information technology resources at college is responsible for utilizing these resources in an efficient, ethical, and legal manner and in ways consistent with overall college policy.

Scope

The following principles serve to guide the responsible use of information technology for all the

users of college.

1. Respect the rights of others by complying with all college policies regarding sexual, racial and other forms of harassment, and by preserving the privacy of other individuals. For example, it is prohibited to send harassing messages via email or social networking or transmit or reveal personal or private information individuals.

2. Use computing facilities, accounts and data only when you have appropriate authorization and use them for approved purposes. For example, you should not use Information Technology resources of "St. Mary's PG College Vidisha" to run a business or to access another individual's computer account.

3. Respect all pertinent licenses, contractual agreements and copyrights. Use only legal versions of copyrighted software in compliance with vendor license requirements. Forexample, you should not post another individuals copyrighted material on your web page orinstall software with a single user license on multiple computers.

4. Preserve the integrity of computing systems, electronic data, and communication networks. For example, one should not modify settings on a desktop computer to make it unusable for others or excessively utilize network resources, like music videos, which might overload college network bandwidth.

5. Respect and adhere to all appropriate local, state and government laws. For example, it is prohibited to use IT resources of the college to attack computers on another network by launching viruses, worms, or other forms of attack.

Privacy

While the College values and respects the privacy of its staff, faculty, students, and other users, the intrinsic nature of electronic records limits the extent to which the College can guarantee a user's privacy. Despite security protocols, communications over the Internet—and across the local campus

network of the college—can be vulnerable to interception and alteration. Consequently, theCollege cannot assure that absolute privacy can be maintained for data that resides on the College network or on storage media.

Out of respect for personal privacy, the College does not routinely examine the contents of data or files in user accounts. However, on occasion, circumstances may require an examination of a user's files to maintain system security, to administer or maintain system integrity, to access necessary College information or in response to legal mandate. In such cases, authorized personnel may examine a user's data without notice. Authorized personnel are those specifically entrusted and approved by the College Principal.

Personal Use

Personal use is defined as the non-academic, non-administrative use of IT systems of the college. Such use is solely discretionary; it neither serves an essential employment function nor is it related to academic discourse. Data that result from personal use are "personal data".

Personal use of IT resources of the college is secondary for performing essential College functions using such resources. If personal use of College IT resources interferes with or causes disruptions to the essential functions of the College performed by IT, then authorized personnel may curtail such use.

Passwords and User IDs

System accounts, passwords, and user IDs plays an important role in protecting the files and privacy of all users. Because users are responsible for all uses made of their accounts, users must take exceptional care to prevent unauthorized use of their accounts. This includes changing passwords regularly and disabling "automatic" log-ins.

In most cases, it is inappropriate—and perhaps dangerous—to allow another person to use another user's network credentials or email account. In some cases, a user's data are vulnerable to alteration

or deletion. In others, the validity of a user's credentials could be compromised. Alternatively, if criminal activity can be traced to a user's account, the person to whom the accountis assigned may be held accountable. The College, therefore, reserves the right to restrict or prohibit password sharing.

Data Storage and Back-ups

The College maintains a centralized repository of data stored in user accounts on the College network. This includes all the data that a user creates and saves on the College's network storage devices. It also includes saved email messages, attachments, files, and folders.

The College reserves the right to restrict the amount of network storage available for users. This includes the prerogative to impose quotas on the number and/or size of stored files.

Data files are routinely backed up on a daily, weekly, monthly, and/or yearly basis. These back-ups facilitate the restoration of College data that have been lost, altered, or damaged. The College will not routinely retrieve backed-up personal data. Users, therefore, are encouraged to maintain independent back-ups of their important personal data, including email messages. St. Mary's PG College Vidisha disclaims any responsibility for maintaining or providing access to backups of a user's personal data.

In case of data backed up by the IT department, retrieval or restoration of the same will be the discretion of the Principal.

Security

The College implements appropriate "industry-standard" practices concerning the security of the IT resources of the college. These methods are designed to protect against unauthorized access, intrusion, or damage to the availability, access, or integrity of the IT systems of the college. However, primarily due to the nature of security threats and the remote possibility of a breach of security, the College warrants neither a user's privacy nor the integrity of data stored on the College network (since the College has already adhered to all the industry norms of standards of security)

Copyright, Trademark, and Domain Names

Users must comply with all copyright, trademark, and other intellectual property laws. In general, permission is necessary for a user to reproduce materials, such as video, music, images, or text. To "reproduce" in this context includes downloading and saving a digital copy to a hard drive or other storage media. Photocopying copyrighted materials without authorization is also prohibited.

In addition, users must generally obtain permission from the copyright owner to prepare derivative works, including modifying existing works. Copyright law also prohibits the distribution, display, or performance of works created by another without a proper release.

Compliance and Enforcement

All users of IT resources of the college must abide by these policies. Users not wishing to agree to and comply with this policy will be denied use of or access to IT resources of St Mary's.

College community users who intentionally violate these policies are subject to disciplinary action by the College, in line with the duly established processes of the College. On the discretion of the Principal the alleged violations of this IT policy may be referred to the College disciplinary body. In addition, the Principal may conduct an investigation regarding the alleged infraction. Violators may also be liable for civil damages and/or criminal prosecution, if applicable.

Guest users of publicly available IT resources of the college are also subject to the terms of this policy. While explicit acceptance of this policy is not required for guests to access these limited IT resources, guests are accountable for their actions while using College IT resources. Guests who violate this policy will be asked to cease use and may be barred from further access.

Members of the "St. Mary's PG College Vidisha" community who believe they have witnessed or been a victim of a violation of this policy should notify or file a complaint with the appropriate authority at the College office. Students should report suspected violations to the Class Counselor. Faculty members should report suspected violations to the Vice Principal. Staff members should

report suspected violations to their department head that may further report the problem to the Discipline Committee. Reports of suspected unauthorized use or misuse of "St. Mary's PG College Vidisha" information technology resources would be investigated pursuant to standard College procedures.

II Data Security Policy

Purpose

This policy defines the guidelines for the security and confidentiality of data maintained St. Mary's PG College Vidisha both in paper and electronic form. This policy also informs each person who is entrusted to access student, employee and/or institutional data of their responsibilities with regard to confidentiality and safeguarding the data of St. Mary's PG College Vidisha.

Statement of Policy

All custodians and guardians of administrative data are expected to manage, access, and utilize the data in a manner that maintains and protects the security and confidentiality of that information. All notice to the Government of India, State & local regulations must be considered and adhered to when using or sharing personal or confidential information. Any notice of a breach of confidential information whether in paper or electronic form must be reported to the Principal.

Under no circumstances shall credit card numbers be stored or sent from College servers or desktops.

Scope

College employees, or others who are associated with the college, who request, use, possess, orhave access to college administrative data must agree to adhere to the protocols outlined in the general IT policy.

Changing data of oneself or others except as required to fulfill one's assigned College duties or asauthorized by a supervisor. (This does not apply to self-service applications that are designed to permit you to change your own data).

- Disclosing information about individuals without prior authorization by the college administration.
- Engaging in what might be termed "administrative voyeurism" (reviewing information not required by job duties) unless authorized to conduct such analyses. Examples include tracking the pattern of salary raises, viewing a colleague's personal information, looking up someone else's grades or viewing another colleague's work product when not authorized to do so.
- Circumventing the level of data access given to others by providing access that is broader than that available to them, unless authorized. For example, providing an extract file of employee salaries to someone who does not have security access to salary data is prohibitedby this policy.
- Allowing unauthorized access to College's administrative systems or data by sharing an individual's username and password.
- Engaging in any other action that violates the letter and spirit of this policy, either purposefully or accidentally.

III Electronic Communication Policy

Purpose

St. Mary's PG College Vidisha has invested in its technology

infrastructure to enhance teaching and learning and to enable efficient business practices. Student, faculty, and staff members have access to email, LMS and other apps as a communication tool for current news, events, personalized messages and teaching and learning activities. The College is committed to theuse of College wide electronic communication to enhance interpersonal communications, improve information exchange, and to reduce the use of paper and printed materials.

The purpose of this policy is to identify electronic communication as an official means of communication within St. Mary's PG College Vidisha and to define the responsibilities of college students, faculty and staff related to electronic communication.

Statement of Policy

St. Mary's PG College Vidisha provides access to email /LMS for all faculty/ students and staff. Email is an official method of communication at College. Students, faculty and staff are held strictly responsible for the consequences of not reading College relatedcommunications sent to their official e-mail address.

IV Personal Digital Assistant Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the use and support of Personal Digital Assistant devices (PDAs) that are common in the workplace and maybe used by employees of St. Mary's PG College Vidisha. This policy applies to, but is not limited to, all devices thatfit the following device classifications:

Handhelds running the Apple OS, Android OS, Blackberry OS, Palm OS, Microsoft WindowsCE, Pocket PC, Windows Mobile, Symbian,

or Mobile Linux operating systems and others.

Mobile devices that are wireless or wired (i.e. connectible using the College wired or wirelessnetwork or by a wireless provider network such as Verizon, ATT or Sprint.

Smartphones that include PDA functionality.
Any third-party hardware, software, processes, or services used to provide connectivity to theabove.

The policy applies to any PDA hardware and related software that could be used to access college resources, even if the equipment is not sanctioned, owned, or supplied by the college. The overriding goal of this policy is twofold.

The first goal is to protect the technology-based resources of the College (such as College data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attacks that could result in loss of information, damage to critical applications, loss of revenue or damage toour public image.
The second goal of this policy is to make clear the limits that the College places on user support for PDA devices.

Scope

This policy applies to all employees and students (including full and part-time staff), contractors, and other agents of St. Mary's PG College Vidisha who utilize College-owned, personally-owned, or publicly-accessible PDA-based technology to access the College's data and networks via wired or wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at St. Mary's PG College Vidisha does not automatically guarantee the granting of these privileges.

Addition of new hardware, software, and/or related components to provide additional PDA-related connectivity within College facilities will be managed at the sole discretion of the Information Technology Department and the College.

Supported Technology

At this time St. Mary's PG College Vidisha does not provide support for employee owned Cell Phones or PDAs. St. Mary's PG College Vidisha IT Department is not able to provide personal consulting to individual employees, other than providing a best effort attempt to assist an employee in their own attempt at connecting a PDA device to a College IT resource. Such support is limited to time available and will often require the employee to perform upgrades, patches and revisions on their own.

Policy and Appropriate Use

It is the responsibility of any employee and student of St. Mary's PG College Vidisha who is connecting to the College's network via a PDA to ensure that all components of his/her connection remain as secure as his/her network access within the office. It is imperative thatany wired (via sync cord, for example) or wireless connection, including, but not limited to PDA devices and service, used to conduct St. Mary's PG College Vidisha business be utilized appropriately, responsibly, and ethically. Failure to act accordingly may result in immediate suspension of that user's account at the sole discretion of the IT Department. Based on this, the following rules should be observed:

1. Employees using PDAs and related software to connect to technology infrastructure of the college will, without exception, use secure remote access procedures. This will be enforced through public/private key passwords in accordance with College's *General IT policy*. Employees agree to never disclose their passwords to anyone, including family

members if college work is conducted from home.

2. St. Mary's PG College Vidisha IT Department reserves the right to require students and employees to shut down any form of personally owned technology that has been identified to causeinterference with the proper functioning of the College wireless technology.

3. Any PDA that is configured to access St. Mary's PG College Vidisha resources via wireless or wired connectivity must adhere to the authentication requirements of the College, asfound in the Data Security policy and the Responsible Use policy.

4. Employees, contractors, temporary staff and students will make no modifications of any kind to College-owned and installed hardware or software without the approval of the IT Department. Thisincludes, but is not limited to, installation of PDA software on College-owned desktop or laptop computers, connection of sync cables and cradles to College-owned equipment, and use of the College's wireless network bandwidth via these devices.

10. The IT Department reserves the right to suspend without notice any access port to the network that puts the College's systems, data, users, and clients at risk.

Security

1. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain college data. Any non-college computer used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by the IT Department. Anti-virus signature files on any additional client machines – suchas a

home PC – on which this media will be accessed, must be up to date.

3. Passwords and other confidential data as defined by the IT Department are not to be stored unencrypted on mobile devices.

4. Any mobile device that is being used to store the data St. Mary's PG College Vidisha must adhere to the authentication requirements of the College. In addition, all hardware security configurations (personal or College-owned) must be pre-approved by the IT Department before any enterprise data-carrying device can be connected to it.

5. The IT Department will manage security policies, network, application, and data access centrallyusing whatever technology solutions it deems suitable. Any attempt to disable or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with College's Responsible Use policy.

6. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase College-specific data from such devices once their use is nolonger required.

Help & Support

1. The IT department will support its sanctioned hardware and software, but is not responsible or accountable for conflicts or problems with personally owned PDA devices or other hardware and software.

2. The IT Department reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the College network.

3. The IT Department will provide support (limited) to the College email communications application only. This includes email, calendar, and

contacts.

4. The College cannot be held responsible for damage or loss of information on a personal PDA device when, at the request of the owner, it is being supported by a representative of the IT Department.

V Wireless Network Policy

Purpose

St. Mary's PG College Vidisha provides wireless networking services in campus to enable the convenience of Internet connectivity. This service allows members of the College communityto access the campus wide network from wireless devices or portable computers where coverage is available.

The purpose of this policy and related procedures is to define responsibilities for the management and use of the wireless network and to manage other uses of the wireless spectrum and to ensure security across the "St. Mary's PG College Vidisha" network.

Scope

The IT Department will regulate and manage all wireless access points used by wireless technologyto ensure fair and efficient allocation and to minimize collision, interference, unauthorized intrusion and failure of the wireless network.

DEFINITIONS

Access Point (AP)

A hardware device that acts as a communication hub for users of a wireless device to connect to a wired network. APs are important for

providing heightened wireless security and for extending the physical range of service to which a wireless user has access.

Wireless device

The end user system or device that accesses the wireless network for data communications purposes. This is normally a portable computer (Laptop) or personal digital assistant (PDA) containing an appropriate wireless network interface card (NIC).

PROCEDURES

Security

Users should assume that data transmitted over the wireless network is NOT secure.

Access Points

Only access points provided and installed by the IT Department or approved for installation by IT are permitted on the College network. IT reserves the right to disconnect and remove any access point not installed and configured by IT personnel or specifically covered by prior
written agreement and/or arrangement with IT. In cases where the device is being used for specific academic or research applications IT will work with faculty to determine how the wireless devices may be used while maintaining required security and without causing interference. Any person found responsible for the installation of unauthorized access points may be submitted to the appropriate college authority for disciplinary action. All access points shall be installed and configured in such a way as to comply with all security features of the wireless network, including restrictions to

provide connections only to those users who are authorized to access the "St. Mary's PG College Vidisha" network.

Other Wireless Devices

Unapproved wireless devices, such as portable phones and other devices with two-way radios may interfere with the operation of the College wireless network. If the IT departmentreceives a report of interference and determines that a non-approved wireless device is causing interference with the College functioning, it reserves the right to ask the owner of the device to discontinue its use.

Authorized Use

Only users affiliated to St. Mary's PG College Vidisha, are authorized to use wireless networking on campus. IT may implement or alter data encryption and authenticationsecurity measures at any time with the proper notification to the community. All users to provide security to "St. Mary's PG College Vidisha" network users and electronic resources must follow these measures. These measures require the use of specific wireless network products and are designed to meet emerging wireless encryption and security standards. These measures may include other authentication mechanisms including authorization by username and password.

ALL THE ABOVE POLICY APPLIES TO:

This policy applies to all students, faculty, and staff of St. Mary's PG College Vidisha and to all other IT users of the "St. Mary's PG College Vidisha". These users are responsible for reading, understanding, and complying with this policy.

Director
(Fr.Selvichan John)