Bharatiya Shikshan Prasarak Sanstha, Ambajogai

Swa. Sawarkar Mahavidyalaya, Beed

Internal Quality Assurance Cell

Criteria 6- Governance, Leadership & Management

Key Indicator 6.2: Strategy Development & Deployment

6.2.1: ***The institutional perspective plan is effectively deployed and functioning of the institutional bodies is effective and efficient as visible from policies, administrative setup, appointment, service rules, and procedures, etc.***

IT Administration Policy

IT ADMINSTRATION POLICY

Policy Title : IT ADMINSTRATION POLICY		
1.	Administrative Policy Number (APN): 02/IT/2019-20	01/02/2019
2.	Brief Description of the Policy	IT related infrastructure and Procurement and Maintenance
3.	Drafting	CDC / IQAC
4.	Policy applies to	**Staff and Students**
5.	Effective from the date	01/06/2019
6.	Approved by	CDC,Principal
7.	Responsible Authority	IQAC
8.	Superseding Authority	Principal
9	Last Reviewed /Updated	---
10	Main Objective of the Policy	1. Timely Review of Requirement ,Planning for procurement and Maintenance of the IT infrastructure of the college. 2. To provide IT Facilities to assist staff students and other authorized users to conduct bonafide academic and administrative pursuits. 3. To ensure that all users must accept full responsibility for using the IT facilities in an honest , ethical and legal manner and with regard to the privacy , rights and sensitivities of other people .

Dr. R. M. Dhere
Vice Principal & IQAC Co-ordinator
Swa.Sawarkar Mahavidyalaya, Beed

Principal
Swa.Sawarkar Mahavidyalaya
Beed.

		4. To make the system administrator and user aware and responsible for the protection of the IT network. 5. To facilitate an effective availability of network at all times and rapid tracking down and resolution of any network problems. 6. To Minimize interruptions in the IT Services.

IQAC Coordinator

Dr. R. M. Dhere
Vice Principal & IQAC Co-ordinator
Swa.Sawarkar Mahavidyalaya, Beed

Principal

Principal
Swa.Sawarkar Mahavidyalaya
Beed.

Contents

Introduction

All possible information technologies for the quality improvement of teaching learning at The Swa Sawarkar Mahavidyalaya Beed. 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 Swa.Sawarkar Mahavidyalya 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 support 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 .
- 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.
- 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 .
- colleges to support resource sharing, up gradation, and continuing education of teachers; guidance, counseling and academic support to students;
- Resource sharing, management and networking of college managers in improved efficiencies in the teaching-learning process.

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.

IT Policy

The IT Policy of the College is as follows

I General IT Ethics / Ethos Policy

Purpose

College 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.

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

Statement of Policy

College 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 Swa. Sawarkar Mhavidyalaya to run a business or to access another individual's computer account.

3. 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.

4. 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, the College cannot assure that absolute privacy can be maintained for data that resides on the College network or on storage media.

Personal Use

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 account is assigned may be held accountable. The College, therefore, reserves the right to restrict or prohibit password sharing.

Data Storage and Back-ups

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.

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.

Compliance and Enforcement

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.

II Data Security Policy

Purpose

This policy defines the guidelines for the security and confidentiality of data maintained by The College 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 College.

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.

Scope

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

III Electronic Communication Policy

Purpose

The College 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 the use of College wide electronic communication to enhance interpersonal communications, improve information exchange, and to reduce the use of paper and printed materials.

Statement of Policy

The College 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 related communications sent to their official e-mail address.

Scope

Assigning of institutional email ID

Faculties and staff are assigned an email username and password upon acceptance to a program or upon hire. Core faculty, Coordinators and staff are assigned an additional username and password upon hire by the College,. The official college email address is:

Faculty/Staff - **username@sawarkarcollegebeed .edu.in**

G-suite : admin@sawarkarcollegebeed.edu.in

Educational uses of electronic communications

Faculty members may require the use of email or other forms of electronic communication

Responsible use of email

Email, G suite are the tool provided by the College to complement traditional methods of communications and to improve education and administrative efficiency. All email users have a responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the college's e-mail system is confirmation that the user agrees to be bound by this policy. Violations of the policy may result in restriction of access to the College's email system and/or other appropriate disciplinary action.

Individuals are responsible for saving email messages as they deem appropriate. Due to limited resources the IT department has the right to restrict the amount of user storage on the College email system. Google likewise controls G-suit email storage quotas. Users are asked

to manage the volume of email in their account and are required, from time-to-time, to purge deleted or trashed emails. The College reserves the right to purge deleted emails in a users' account if space needs become critical.

The following types of emails are explicitly prohibited:

- Emails that knowingly transmit a message containing a computer virus.
- Emails that intentionally misrepresent the identity of the sender of e-mail.
- Emails that use or attempt to use the accounts of others without their permission.

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 may be used by employees of College. This policy applies to, but is not limited to, all devices that fit the following device classifications:

Handhelds running the Apple OS, Android OS, Blackberry OS, Palm OS, Microsoft Windows CE, PocketPC, 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 wireless network 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 the above.

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 to our public image.

Supported Technology

The College 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

1. Employees using PDAs and related software to connect to technology infrastructure of the college will, without exception, use secure remote access procedures.

2. 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. This includes, 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.

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

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

3. Any mobile device that is being used to store the data of The Bhopal School of Social Sciences, Bhopal 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.

4. The IT Department will manage security policies, network, application, and data access centrally using 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.

5. 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 no longer required.

Help & Support

1. College's 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.

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

5. 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

The College provides wireless networking services in campus to enable the convenience of Internet connectivity. This service allows members of the College community to 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 "Swa. Sawarkar Mahavidyalaya" network.

Scope

The IT Department will regulate and manage all wireless access points used by wireless technology to 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 .

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.

Authorized Use

College is authorized to use wireless networking on campus. IT may implement or alter data encryption and authentication security measures at any time with the proper notification to the community. All users to provide security to "**Swa.Sawarkar Mahavidyalaya** " 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 Swa. Sawarkar Mahavidyalaya and to all other IT users of the "College ". These users are responsible for reading, understanding, and complying with this policy.

Dr. R. M. Dhere
Vice Principal & IQAC Co-ordinator
Swa.Sawarkar Mahavidyalaya, Beed

Principal
Swa.Sawarkar Mahavidyalaya
Beed.