

# Parvatibai Chowgule College of Arts and Science

## Margao-Goa

### IT Policy

#### INTRODUCTION

Commensurate with our Mission statement “We at Chowgule College are committed to excellence in education, empowering personalities and developing responsible members of society”, it is the purpose of this Executive Memorandum to set forth the administrative policy of Parvatibai Chowgule College and provide guidance relating to responsible use of the College’s electronic information system.

#### GENERAL

Access to electronic information systems at the Parvatibai Chowgule College is a privilege, not a right, and must be treated as such by all users of these systems. All users must act honestly and responsibly. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements related to Parvatibai Chowgule College information systems. All users shall act in accordance with these responsibilities, and there levant local and state laws and regulations. Failure to so conduct oneself in compliance with this Policy may result in denial of access to Parvatibai Chowgule College information systems or other disciplinary action.

#### OBJECTIVE AND PURPOSE

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic mission of the college in teaching, learning, research and administration. The Policy therefore aims to promote the following goals:

To ensure the integrity, reliability, availability and superior performance of IT systems.

To ensure the use of IT systems is consistent with the principles and values that govern use of other College facilities and services.

To ensure that IT systems are used for their intended purposes

To establish processes for addressing policy violations and sanctions for violators.

## SCOPE

This Policy applies to all Users of IT Systems, including but not limited to College students, faculty, and staff. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by ITS, as well as those administered by individual departments, College laboratories, and other College-based entities. Use of IT Systems, even when carried out on a privately owned computer that is not managed or maintained by Parvatibai Chowgule College, Margao, is governed by this Policy.

## DEFINITIONS

For the purpose of this Policy, the following definitions shall apply:

**[IT Systems]** These are the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and datafiles that are owned, managed, or maintained by Chowgule College. For example, ITSystems include institutional and departmental information systems, faculty research systems, desktop computers, the College campus network, and College general access computer clusters.

**[User]** A "User" is any person, whether authorized or not, who makes any use of anyIT System from any location. For example, Users include a person who accesses ITSystems in a University computer cluster, or via an electronic network.

**[Systems Authority]** While Chowgule College is the legal owner or operator of all ITSystems, it delegates oversight of particular systems to the head of a specificsubdivision, department, or office of the College ("Systems Authority"), or to an individual faculty member, in the case of IT systems purchased with research or other funds for which he or she is personally responsible.

**[Systems Administrator]** Systems Authorities may designate another person as"Systems Administrator" to manage the particular system assigned to him or her. The Systems Administrator oversees the day-to-day operations of the system and is authorized to determine who is permitted access to particular IT resources.

**[Certifying Authority]** This is the Systems Administrator or other College authority that certifies the appropriateness of an official College document for electronic publication in the course of College business.

**[Specific Authorization]** This means documented permission provided by the applicable Systems Administrator.

**[Electronic Communications]** shall mean and include the use of information systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, World Wide Web (Internet), or other such electronic tools.

**[Information Systems]** shall mean and include computers, networks, servers and other similar devices that are administered by the College and for which the Collegeis responsible. "Networks" shall mean and include video, voice and data networks,routers and storage devices.

**[Obscene]** with respect to obscene material shall mean (1) that an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity,

sex, or excretion, (2) the material depicts or describes in a patently offensive way sexual conduct (3) the material taken as a whole lacks serious literary, artistic, political, or scientific value. (4) the material encourages / promotes religious fanaticism /propaganda or anti-social behavior.

### PERMITTED USE

a. The College Information Systems are to be used predominately for University and College related purposes. However, personal use is permitted so long as it conforms to this Policy and does not interfere with College operations or an employee user's performance of duties as a College employee. As with permitted personal use of telephones for local calls, limited personal use of

information systems does not ordinarily result in additional costs to the College and may actually result in increased efficiencies. Personal use of any College information system to access, download, print, store, forward, transmit or distribute obscene material is prohibited.

UNDER ALL CIRCUMSTANCES, PERSONAL USE BY EMPLOYEES MUST COMPLY WITH SUBSECTION b. OF THIS SECTION AND SHALL NOT CONFLICT WITH AN EMPLOYEE'S PERFORMANCE OF DUTIES AND RESPONSIBILITIES FOR THE COLLEGE.

Personal use may be denied when such use requires an inordinate amount of information systems resources (e.g. storage capacity).

b. Prior Approval Required for Personal Use for Outside Consulting, Business or Employment. Personal use of College information systems resources or equipment by any user for personal financial gain in connection with outside (non-College) consulting, business or employment is prohibited. Employee personal use in conjunction with outside professional consulting, business or employment activities is permitted only when such use has been expressly authorized and approved by the College Administration or the Management of the College.

### RESPONSIBILITIES

**For any Assistance the following is the information:**

1. Office of Information Technology (OIT) at Parvatibai Chowgule College

2. OIT Help Desk

**Facilities:**

**[IT-Policy]** One has to Sign the online IT-Policy located on <http://www.chowgules.ac.in>; in order to access the Chowgule College, IT Infrastructure.

**[Computer Labs]** All authorized users are requested to use their Department Computer Lab.

**[Hardware / Software]** Every faculty is given an access point as per the department policies.

**[Printing & Scanning]** As per College policies.

### Policy on Chowgule College Academic Area Network

1. Office of Information Technology (OIT) is responsible for the core Chowgule College network (includes Internet facilities: email, web etc).

2. Office of Information Technology (OIT) will provide connectivity to each Department, to the gigabit backbone, and also the necessary IP addresses, proxies, email relays etc.

3. The operation of the network within each Department is the sole responsibility of the Department Head and OIT will only play an advisory role.

4. Installation of hardware/software, setting up and configuration, virus cleaning, maintenance and upkeep of residential computers is the sole responsibility of the residents of the department. In case, a particular department cannot perform the following task, OIT should perform this task to ensure that all systems are updated and maintained.

5. If a Department network "misbehaves" and causes problems for any other department or the entire campus, or disrupts services, the Head will notify OIT and the Systems Administrator can disconnect the Department from the core network until the problem is fixed satisfactorily. System Administrator should notify the Department (Staff as well as Students) before proceeding with any maintenance activities.

6. Use of pirated/illegal software is not acceptable. It is the responsibility of the Departments Heads and Systems Administrator to ensure compliance.

7. It is the responsibility of the Systems Administrator to ensure that all systems in all departments are protected against harmful viruses and other services that may

be disrupt the security of the existing networks present in the campus. All departments should MANDATORILY have, both, authorized antivirus and firewalls setup on the systems and the Systems Administrator should ensure compliance.

8.It is the responsibility of the System Administrator to document the network infrastructure for maintenance purposes of the entire campus. All activities such as number of users, number of networks, periodic reports of virus scanning, traffic generated over network, the bandwidth available and its proper allocation etc should also be documented and submitted to the Head of the Institution, at the most, once in the month. Diagrammatic Models should be provided wherever necessary in the documentation.

9.OIT is responsible for allocating and controlling the available bandwidth to all departments and should ensure the appropriate bandwidth is available to all departments depending on the usage requirement as per the department. OIT staff and System Administrator are not permitted to restrict the bandwidth for personal use in which the Head of the Institution will take strict action.

#### Policy on Help, Complaints and Requests

#### **Departments**

- 1.The System Administrator should resolve password issues.
- 2.System Administrator should add new Student, Staff etc.
- 3.Logins once changed cannot be renamed.

Note that posting complaints only on the newsgroups may not receive a response. So please register complaints at the right place to get a prompt response.

#### **How to log a request / complaint (in order of preference)**

1.The following details are to be sent by email whenever any problem is encountered to the OIT:

- a. Name, Class, Roll no, email id

b. Brief description of the problem

2.You may log your request in a register kept in the OIT. This facility is available only on working days and timings i.e. when the office is open.

**Guidelines for use of newsgroups hosted by OIT**

- 1.Please post material that is consistent with the title of the newsgroup.
- 2.Ensure that your mails are polite and follow netiquette accepted by the Chowgule College community.
- 3.Do not make postings related to materials or topics that are considered unlawful or unacceptable to the Chowgule College community. In particular, hate speech and slander are forbidden.
- 4.Advertising and exchange offers for items of commercial value or those not considered legal is prohibited.
- 5.Postings must be made from genuine Ids and not from aliases.

Penalties for not following these guidelines may include: banned from posting to newsgroups, removal of access to the Chowgule College network and a complaint to the College Principal.

**Information for STUDENTS/FACULTY leaving Parvatibai Chowgule College**

This is regarding your college account login and your email address of the form(user@chowgules.ac.in). OIT will keep this address as a forwarding address for you. But the following things will not work from the time you cease to be a student of the college. i.e. Once the name is no longer on the college rolls:

- 1.Email authentication will not succeed.

2.The email storage space will be removed. Do take a backup of any important data that you have there.

## POLICY SECTIONS

### **Appropriate use of IT Systems**

Although this Policy sets forth the general parameters of appropriate use of IT Systems, faculty, students, and staff should consult their respective governing

policy manuals for more detailed statements on permitted use and the extent of use that the College considers appropriate in light of their varying roles within the community. In the event of conflict between IT policies, this Appropriate Use Policy will prevail.

**A.[Appropriate Use]** IT Systems may be used only for their authorized purposes -- that is, to support the research, education, clinical, administrative, and other functions of Chowgule College. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

**B.[Proper Authorization]** Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

**C.[Specific Proscriptions on Use]** The following categories of use are inappropriate and prohibited:

1.Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages).Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. Use that is inconsistent with College's non-profit status. The College is a non-profit, tax-exempt organization and, as such, is subject to specific state, and local laws regarding sources of income, political

activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-Chowgule College purposes is generally prohibited, except if specifically authorized and permitted under the College's conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the College's educational,

administrative, research, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. Use of IT Systems in a way that suggests College endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes College involvement, except for authorized lobbying through or in consultation with the College Office.

4. Harassing or threatening use: This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.

5. Use damaging the integrity of Chowgule College or other IT Systems. This category includes, but is not limited to, the following six activities:

a. Attempts to defeat system security. Users must not defeat or attempt to defeat any IT.

b. System's security – for example, by "cracking" or guessing and applying the identification or password of another User. (This provision does not prohibit, however, the System Administrator from using security scan programs within the scope of their Systems Authority).

c. Unauthorized access or use: The College recognizes the importance of preserving the privacy of Users and data





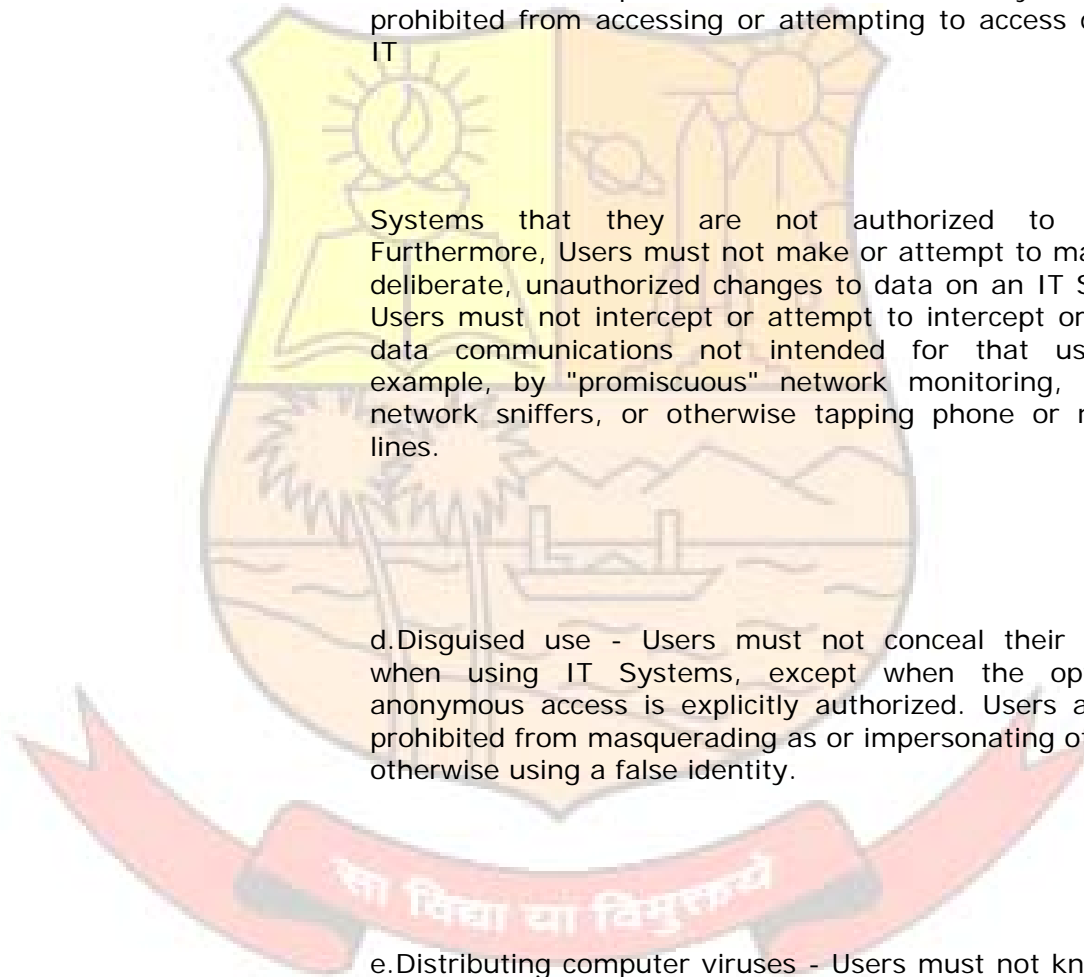
stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Chowgule organization or individual may not use non-public IT Systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Chowgule College organizations or individuals across the College network without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT

Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

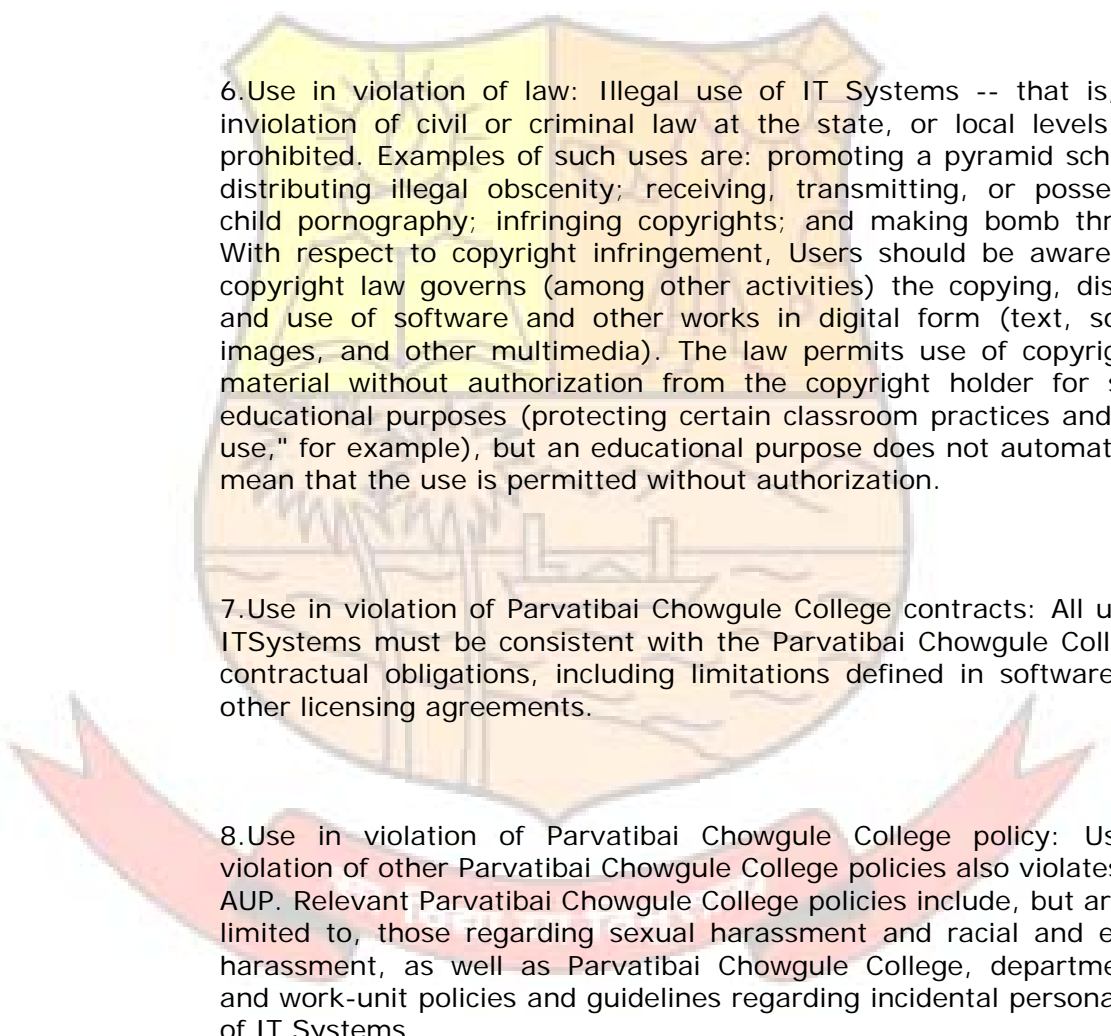
d. Disguised use - Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

e. Distributing computer viruses - Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

f. Modification or removal of data or equipment - Without specific authorization, Users may not remove or modify any College-owned or administered equipment or data from IT Systems.



g. Use of unauthorized devices. Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.



6. Use in violation of law: Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats. With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

7. Use in violation of Parvatibai Chowgule College contracts: All use of IT Systems must be consistent with the Parvatibai Chowgule College's contractual obligations, including limitations defined in software and other licensing agreements.

8. Use in violation of Parvatibai Chowgule College policy: Use in violation of other Parvatibai Chowgule College policies also violates this AUP. Relevant Parvatibai Chowgule College policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as Parvatibai Chowgule College, departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.

9. Use in violation of external data network policies. Users must observe all applicable policies of external data networks when using such networks.

**D. [Personal Account Responsibility]** Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes

of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

**E. [Repair and Maintenance of Equipment and Software]** Users should be aware that on occasion duly authorized Parvatibai Chowgule College information systems technological personnel have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment the Parvatibai Chowgule College deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for Parvatibai Chowgule College needs. Information systems technological personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them. The Programmers of the College will do the maintenance of the Software like Admission, Examination, etc. and any other work given by the Principal from time to time.

**F. [Procurement of Software]** A duly constituted committee of the college will do this.

**G. [Encryption of Data]** Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks.

**H. [Responsibility for Content]** Official College information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document. Users also are able to publish information on IT Systems or over College's networks. Neither the College nor the System Administrator can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The College will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private speech of an individual user.

**I. [Personal Identification]** Upon request by the System Administrator or other Parvatibai Chowgule College authority, Users must produce valid Parvatibai Chowgule College identification.

## CONDITIONS OF ACCESS

The College places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the College may determine that certain broad concerns outweigh the value of a User's expectation of privacy and warrant College access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relation with the Parvatibai Chowgule College, his or her ID and password shall be denied further access to College computing resources.

**A. [Conditions]** The College may access all aspects of IT Systems, without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or
2. When required by state, or local law or administrative rules; or
3. When there are reasonable grounds to believe that a violation of law or a significant breach of College policy may have taken place and access and inspection or monitoring may produce evidence related to them is conduct; or
4. When such access to IT Systems is required to carry out essential business functions of the College; or
5. When required to preserve public health and safety.

**B. [Process]** Consistent with the privacy interests of Users, College access without the consent of the User will occur only with the approval of the Principal and Head (for faculty users as appropriate (for student users), or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The College, through the Systems Administrator, will log all instances of access without consent. Systems Administrator will also log any emergency entry within their control for subsequent review by the Principal.

**C.[User Access Deactivations]** In addition to accessing the IT Systems, the College, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user

services, or data. The Systems Administrator will attempt to notify the User of any such action.

**D.[Use of Security Scanning Systems]** By attaching privately owned personal computers or other IT resources to the College's network, Users consent to College use of scanning programs for security purposes on those resources while attached to the network.

**E.[Logs]** Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. The Systems Administrator is required to establish and post policies and procedures concerning logging of User actions, including the extent of individually identifiable data collection, data security, and data retention.

**F.[Encrypted Material]** The College may access encrypted files, documents, and messages.

## WEB PAGES

The Central Administration at the campus may establish standards for those WebPages considered to be "official" pages of the Parvatibai Chowgule College. All official WebPages shall contain the administrative unit's logo in the header and footer in order to identify it as an official Parvatibai Chowgule College of Web Page. No other Web Pages shall be allowed to use Parvatibai Chowgule College of Chowgule College logos without the express permission of the Parvatibai Chowgule College. Originators of all Web Pages using information systems associated with the Parvatibai Chowgule College shall comply with Parvatibai Chowgule College policies and are responsible for complying with all state and local laws and regulations, including copyright laws, obscenity laws, laws relating to libel, slander and defamation, and laws relating to piracy of software. The person creating a Web Page are responsible for the accuracy of the information contained in the Web Page. Content should be reviewed on a timely basis to assure continued accuracy. Web Pages should include a phone number or e-mail address of the person to whom questions/comments may be addressed, as well as the most recent revision date. The Web Pages should also provide FAQ's and all college related activities/information from time to time.

## ENFORCEMENT PROCEDURES

**A.[Complaints of Alleged Violations]** An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established College Grievance Procedures(including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the Principal's Office, which must investigate the allegation and (if appropriate)refer the matter to College disciplinary and/or law enforcement authorities.

**B.[Reporting Observed Violations]** If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the Principal's Office, which must investigate the allegation and (if appropriate) refer the matter to College disciplinary and/or law enforcement authorities.

**C.[Disciplinary Procedures]** Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students as per college regulations. The System Administrator may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, the Systems Administrator is authorized to investigate alleged violations.

**D.[Penalties]** Individuals found to have violated this Policy may be subject to penalties provided for in other College policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The applicable disciplinary authority in consultation with the Systems Administrator shall determine the appropriate penalties.

**E.[Legal Liability for Unlawful Use]** In addition to College discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

**F.[Appeals]** Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

Incidence that is reported will attract penalties for punitive action by appropriate authorities constituted by the college.

## POLICY DEVELOPMENTS

This Policy must be periodically reviewed and modified by the Provost of the College, who may consult with relevant College committees, faculty, students, and staff.

