Smt. Parvatibai Chowgule College of Arts and Science

Margao-Goa

IT Policy

INTRODUCTION

Commensurate with our Mission statement "We at Chowgule College are committedto excellence in education, empowering personalities and developing responsiblemembers of society", it is the purpose of this Executive Memorandum to set forth theadministrative policy of Smt. Parvatibai Chowgule College and provide guidancerelating to responsible use of the College's electronic information system.

GENERAL

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

OBJECTIVE AND PURPOSE

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

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

To ensure the use of IT systems is consistent with the principles and valuesthat 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 forviolators.

SCOPE

This Policy applies to all Users of IT Systems, including but not limited to Collegestudents, faculty, and staff. It applies to the use of all IT Systems. These includesystems, networks, and facilities administered by ITS, as well as those administeredby individual departments, College laboratories, and other College-based entities.Use of IT Systems, even when carried out on a privately owned computer that is notmanaged or maintained by S.P.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, modembanks, 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 researchsystems, desktop computers, the College campus network, and College generalaccess 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 anindividual faculty member, in the case of IT systems purchased with research orother 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 isauthorized to determine who is permitted access to particular IT resources.

[Certifying Authority] This is the Systems Administrator or other College authoritythat certifies the appropriateness of an official College document for electronicpublication in the course of College business.

[Specific Authorization] This means documented permission provided by theapplicable Systems Administrator.

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

[Information Systems] shall mean and include computers, networks, servers andother 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 personapplying contemporary community standards would find the material taken as awhole predominantly appeals to the prurient interest or a shameful or morbidinterest in nudity, sex, or excretion,

(2) the material depicts or describes in apatently offensive way sexual conduct (3) the material taken as a whole lacks seriousliterary, artistic, political, or scientific value. (4) the material encourages / promotesreligious fanatism /propaganda or anti-social behavior.

PERMITTED USE

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

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

UNDER ALL CIRCUMSTANCES, PERSONAL USE BY EMPLOYEES MUST COMPLYWITH SUBSECTION b. OF THIS SECTION AND SHALL NOT CONFLICT WITH ANEMPLOYEE'S PERFORMANCE OF DUTIES AND RESPONSIBILITIES FOR THECOLLEGE.

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

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

RESPONSIBILITIES

For any Assistance the following is the information:

1.Office of Information Technology (OIT) at S.P.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 DepartmentComputer Lab.

[Hardware / Software] Every faculty is given an access point as per thedepartment 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 ChowguleCollege network (includes Internet facilities: email, web etc).

2.Office of Information Technology (OIT) will provide connectivity to eachDepartment, 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 responsibilityof the Department Head and OIT will only play an advisory role.

4.Installation of hardware/software, setting up and configuration, viruscleaning, maintenance and upkeep of residential computers is the soleresponsibility of the residents of the department. In case, a particulardepartment cannot perform the following task, OIT should perform this taskto ensure that all systems are updated and maintained.

5.If a Department network “misbehaves” and causes problems for any otherdepartment or the entire campus, or disrupts services, the Head will notifyOIT and the Systems Administrator can disconnect the Department from thecore 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 theDepartments Heads and Systems Administrator to ensure compliance.

7.It is the responsibility of the Systems Administrator to ensure that all systemsin all departments are protected against harmful viruses and other servicesthat may be disrupt the security of the existing networks present in thecampus. 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 networkinfrastructure for maintenance purposes of the entire campus. All activitiessuch as number of users, number of networks, periodic reports of virusscanning, traffic generated over network, the bandwidth available and itsproper allocation etc should also be documented and submitted to the Head ofthe Institution, at the most, once in the month. Diagrammatic Models shouldbe provided wherever necessary in the documentation.

9.OIT is responsible for allocating and controlling the available bandwidth to alldepartments and should ensure the appropriate bandwidth is available to all departments depending on the usage requirement as per the department. OITstaff and System Administrator are not permitted to restrict the bandwidth forpersonal 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.SPCC logins once changed ***cannot***be renamed.

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

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

1.The following details are to be sent by email whenever any problem isencountered 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 isavailable 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 theChowgule College community.

3.Do not make postings related to materials or topics that are consideredunlawful 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 notconsidered 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 tonewsgroups, removal of access to the Chowgule College network and a complaintto the College Principal.

Information for STUDENTS/FACULTY leaving S.P.Chowgule College

This is regarding your SPCC account login and your email address of the form(user@chowgules.ac.in). OIT will keep this address as a forwarding address foryou. But the following things will not work from the time you cease to be astudent 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 anyimportant data that you have there.

POLICY SECTIONS

Appropriate use of IT Systems

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

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

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

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

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

1.Use that impedes, interferes with, impairs, or otherwise causes harmto the activities of others. Users must not deny or interfere with orattempt 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 orpostings widely and without good purpose), or "bombing" (flooding anindividual, group, or system with numerous or large email messages).Knowing or reckless distribution of unwanted mail or other unwantedmessages is prohibited. Other behavior that may cause excessivenetwork traffic or computing load is also prohibited.

2.Use that is inconsistent with College's non-profit status. The College isa non-profit, tax-exempt organization and, as such, is subject tospecific state, and local laws regarding sources of income, politicalactivities, use of property, and similar matters. As a result, commercialuse of IT Systems for non-Chowgule College purposes is generallyprohibited, except if specifically authorized and permitted under theCollege’s conflict-of-interest, outside employment, and other relatedpolicies. Prohibited commercial use does not include communicationsand exchange of data that furthers the College's educational,

administrative, research, clinical, and other roles, regardless ofwhether it has an incidental financial or other benefit to an externalorganization.

3.Use of IT Systems in a way that suggests College endorsement of anypolitical candidate or ballot initiative is also prohibited. Users mustrefrain from using IT Systems for the purpose of lobbying thatconnotes College involvement, except for authorized lobbying throughor 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 repeatedunwelcome 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 orattempt to defeat any IT.

b.System's security – for example, by "cracking" or guessing andapplying the identification or password of another User. (Thisprovision does not prohibit, however, the System Administratorfrom using security scan programs within the scope of theirSystems Authority).

c.Unauthorized access or use: The College recognizes theimportance of preserving the privacy of Users and data stored inIT systems. Users must honor this principle by neither seeking toobtain unauthorized access to IT Systems, nor permitting orassisting any others in doing the same. For example, a non-Chowgule organization or individual may not use non-public ITSystems without specific authorization. Privately ownedcomputers 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 Collegenetwork without specific authorization. Similarly, Users areprohibited 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 notintercept or attempt to intercept or access data communicationsnot intended for that user, for example, by "promiscuous"network monitoring, running network sniffers, or otherwisetapping phone or network lines.

d.Disguised use - Users must not conceal their identity when usingIT Systems, except when the option of anonymous access isexplicitly authorized. Users are also prohibited frommasquerading as or impersonating others or otherwise using afalse identity.

e.Distributing computer viruses - Users must not knowinglydistribute or launch computer viruses, worms, or other rogueprograms.

f.Modification or removal of data or equipment - Without specificauthorization, 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, Usersmust not physically or electrically attach any additional device(such as an external disk, printer, or video system) to ITSystems.

6.Use in violation of law: Illegal use of IT Systems -- that is, use inviolation of civil or criminal law at the state, or local levels -- isprohibited. Examples of such uses are: promoting a pyramid scheme;distributing illegal obscenity; receiving, transmitting, or possessingchild pornography; infringing copyrights; and making bomb threats.With respect to copyright infringement, Users should be aware thatcopyright 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 copyrightedmaterial without authorization from the copyright holder for someeducational purposes (protecting certain classroom practices and "fair

use," for example), but an educational purpose does not automaticallymean that the use is permitted without authorization.

7.Use in violation of S.P.Chowgule College contracts: All use of ITSystems must be consistent with the S.P.Chowgule College'scontractual obligations, including limitations defined in software andother licensing agreements.

8.Use in violation of S.P.Chowgule College policy: Use in violation ofother S.P.Chowgule College policies also violates this AUP. RelevantS.P.Chowgule College policies include, but are not limited to, thoseregarding sexual harassment and racial and ethnic harassment, as wellas S.P.Chowgule College, departmental, and work-unit policies andguidelines regarding incidental personal use of IT Systems.

9.Use in violation of external data network policies. Users must observeall applicable policies of external data networks when using suchnetworks.

D. [Personal Account Responsibility] Users are responsible for maintainingthe security of their own IT Systems accounts and passwords. Any Userchanges of password must follow published guidelines for passwords.Accounts and passwords are normally assigned to single Users and are notto be shared with any other person without authorization by the applicableSystems Administrator. Users are presumed to be responsible for anyactivity carried out under their IT Systems accounts or posted on theirpersonal web pages.

E. [Repair and Maintenance of Equipment and Software] Users shouldbe aware that on occasion duly authorized S.P.Chowgule Collegeinformation systems technological personnel have authority to accessindividual user files or data in the process of performing repair ormaintenance of computing equipment the S.P.Chowgule College deems isreasonably necessary, including the testing of systems in order to ensureadequate storage capacity and performance for S.P.Chowgule Collegeneeds. 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 theCollege 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 collegewill do this.

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

H. [Responsibility for Content] Official College information may bepublished in a variety of electronic forms. The Certifying Authority underwhose auspices the information is published is responsible for the content ofthe published document. Users also are able to publish information on ITSystems or over College's networks. Neither the College nor the SystemAdministrator can screen such privately published material nor can theyensure its accuracy or assume any responsibility for its content. The Collegewill treat any electronic publication provided on or over IT Systems thatlacks a Certifying Authority as the private speech of an individual user.

I. [Personal Identification] Upon request by the System Administrator orother S.P.Chowgule College authority, Users must produce validS.P.Chowgule College identification.

CONDITIONS OF ACCESS

The College places a high value on privacy and recognizes its critical importance inan academic setting. There are nonetheless circumstances in which, followingcarefully prescribed processes, the College may determine that certain broadconcerns outweigh the value of a User's expectation of privacy and warrant Collegeaccess to relevant IT Systems without the consent of the User. Those circumstancesare discussed below, together with the procedural safeguards established to ensureaccess is gained only when appropriate.
13

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

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

1.When necessary to identify or diagnose systems or securityvulnerabilities and problems, or otherwise preserve the integrity of theIT 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 asignificant breach of College policy may have taken place and access andinspection or monitoring may produce evidence related to themisconduct; or

4.When such access to IT Systems is required to carry out essentialbusiness functions of the College; or

5.When required to preserve public health and safety.

B. [Process] Consistent with the privacy interests of Users, College accesswithout the consent of the User will occur only with the approval of thePrincipal and Head (for faculty users as appropriate (for student users), ortheir respective delegates, except when an emergency entry is necessary topreserve the integrity of facilities or to preserve public health and safety. TheCollege, through the Systems Administrator, will log all instances of accesswithout consent. Systems Administrator will also log any emergency entrywithin their control for subsequent review by the Principal.

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

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

D.[Use of Security Scanning Systems] By attaching privately ownedpersonal computers or other IT resources to the College's network, Usersconsent to College use of scanning programs for security purposes on thoseresources while attached to the network.

E.[Logs] Most IT systems routinely log user actions in order to facilitaterecovery from system malfunctions and for other management purposes. TheSystems Administrator is required to establish and post policies andprocedures concerning logging of User actions, including the extent ofindividually 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 S.P.Chowgule College. All official WebPages shall contain the administrative unit's logo in the header and footer in order toidentify it as an official S.P.Chowgule College of Web Page. No other Web Pages shallbe allowed to use S.P.Chowgule College of Chowgule College logos without theexpress permission of the S.P.Chowgule College. Originators of all Web Pages usinginformation systems associated with the S.P.Chowgule College shall comply withS.P.Chowgule College policies and are responsible for complying with all state andlocal laws and regulations, including copyright laws, obscenity laws, laws relating tolibel, slander and defamation, and laws relating to piracy of software. The personscreating a Web Page are responsible for the accuracy of the information contained inthe Web Page. Content should be reviewed on a timely basis to assure continuedaccuracy. Web Pages should include a phone number or e-mail address of the personto whom questions/comments may be addressed, as well as the most recent revisiondate. 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 orshe has been harmed by an alleged violation of this Policy may file acomplaint in accordance with established College Grievance Procedures(including, where relevant, those procedures for filing complaints of sexualharassment or of racial or ethnic harassment) for students, faculty, and staff.The individual is also encouraged to report the alleged violation to theSystems Authority overseeing the facility most directly involved, or to thePrincipal'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 otherwiseis aware of a violation of this Policy, but has not been harmed by the allegedviolation, he or she may report any evidence to the Systems Authorityoverseeing the facility most directly involved, or to the Principal’s Office,which must investigate the allegation and (if appropriate) refer the matter toCollege disciplinary and/or law enforcement authorities.

C.[Disciplinary Procedures] Alleged violations of this Policy will be pursued inaccordance with the appropriate disciplinary procedures for faculty, staff, andstudents as per college regulations. The System Administrator may participatein the disciplinary proceedings as deemed appropriate by the relevantdisciplinary authority. Moreover, at the direction of the appropriatedisciplinary authority, the Systems Administrator is authorized to investigatealleged violations.

D.[Penalties] Individuals found to have violated this Policy may be subject topenalties provided for in other College policies dealing with the underlyingconduct. Violators may also face IT-specific penalties, including temporary orpermanent reduction or elimination of some or all IT privileges. The applicabledisciplinary authority in consultation with the Systems Administrator shalldetermine the appropriate penalties.

E.[Legal Liability for Unlawful Use] In addition to College discipline, Usersmay be subject to criminal prosecution, civil liability, or both for unlawful useof any IT System.

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

Incidence that is reported will attract penalties for punitive action by appropriateauthorities 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.