ದಾವಣಗೆರೆ  ವಿಶ್ವವಿದ್ಯಾನಿಲಯ

DAVANGERE UNIVERSITY

Shivagangotri, Davangere-577007 Karnataka.

Policy Document On
INFORMATION TECHNOLOGY

With effect from Jan 2020, Version 1.0

Contents

1 Preamble

Davanagere University (DU) is one of the youngest affiliating types of Universities in Karnataka. It has a jurisdiction of two Districts viz., Davangere and Chitradurga and head quartered at Davangere. Davangere University was established on 18th August 2009 by being carved out of Kuvempu University with a purpose and vision to meet the educational aspirations of the people of this region.

India's success in the area of Information Technology (IT) Software and Related Services over the past decade has been acknowledged globally.

The Information Technology (IT) Policy of the Davangere University defines regulations, rules, and guidelines for proper utilization as well as the effective maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities along with users.

For this purpose the policy has been drafted to effective and efficient use of the term 'IT Assets includes PC or desktop computers, portables and mobile devices, servers, networking devices including wireless networks, Internet connectivity, externalstorage devices and peripherals like printers and scanners and the software associated therewith'. Misuse of these resources may lead to result in unwanted risk and liabilities for the Davangere University. It is, therefore, expected that these resources are usedprimarily for Davangere University related purposes and in a lawful act and ethical professional way.

University ICT (Information Communication Technology) will be using e-Office, HRM, States Scholarship portals, University affiliation, Seva-Sindhu, Sakala, etc, and it's related policies are provided by the Govt. of Karnataka.

2 Necessitate for IT Policy

Basically the University IT policy exists to maintain, secure and ensure legal and appropriate use of Information Technology infrastructure established by the University on the campus.

This policy establishes University-wide strategies and responsibilities for protecting the privacy, honesty, and accessibility of the information assets that are accessed, created, managed, and/or controlled by the University.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information. Undoubtedly, Intranet and Internet services have become most important resources in universities institutions of higher education and research organizations. Realizing the importance of these services, IQAC of Davangere University took initiative in 2020 and established policy for Information Technology in the university. Over the last ten years, not only active users of the network facilities have increased many folds but also the web-based applications increased. This is a welcome change in the university's academic environment. Now, the university has about 270 LAN point connections covering entire campus and expected to reach 500 connections very soon. ICT (Information Communication Technology) Cell has been given the responsibility of maintaining the university's Intranet and Internet services. Internet Unit is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university. Davangere University (DU) is getting its Internet bandwidth from BSNL Leased Line. Total bandwidth availability from BSNL source is one GBPS, can be extended upto 10 GBPS. DU also has got other BSNL Broadband connectivity of 4MBPS from MHRD (NME-ICT).

University when providing access to Internet to their faculties, research scholars, students, and staff, face certain constraints:

1. Limited Internet bandwidth.
2. Limited infrastructure like computers, computer laboratories,
3. Limited financial resources in which faculty, students and staff should be provided

with the network facilities.

4. Limited technical manpower needed for network management. On one hand, resources are not easily available for expansion to accommodate the continuous rise in Internet needs. In addition, uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes/research nor governance of the university. At the outset, we need to recognize the problems related to uncontrolled surfing by the users.
5. Prolonged or intermittent surfing, affecting quality of work
6. Heavy downloads that lead to choking of available bandwidth
7. Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.
8. Confidential information being made public.

With the extensive use of the Internet, network performance suffers in three ways: When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck. When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications. When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems. Too many concurrent users who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available. Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network. Apart from

this, plenty of employee's time will be lost with a workstation being scanned and cleaned of the virus. Emails, unsafe downloads, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untolddamage to information on the network. They can slow down or even bring the network to a halt. Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial. Hence, in order to securing the network, Internet Unit has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway. However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users. As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation.

Policies also serve as blueprints that help the institution implement security measures. An effective security policy is as necessary to a good information security program as a solid foundation to the building. Hence, Davangere University also is proposing to have its own IT Policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, Intranet and Internet access facilities, collectively called"Information Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this university. While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures. Purpose of IT policy is to set direction and provide information about

acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organisation, departments and individuals who are part of university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies. IT policies may be classified into following groups:

1. IT Hardware Installation Policy
2. Software Installation and Licensing Policy
3. Network (Intranet and Internet) Use Policy
4. E-mail Account Use Policy
5. Web Site Hosting Policy 6.University Database Use Policy

Further, the policies will be applicable at two levels:

1. End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
2. Network Administrators

It may be noted that university IT Policy applies to technology administered by the university centrally or by the individual departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorised resident or non-resident visitors on their own hardware connected to the university network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognised Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the university. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the university IT policy. Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted per- mission to use the University's information technology infrastructure, must comply with the Guidelines. Certain violations of IT

policy laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

2.1 Applies to...

Stake holders on campus or off campus

1. Students: UG, PG, PG Diploma, Research scholar, Post-Doctoral/PDF/D.Litt/ D. Sc and Others
2. Employees (Permanent/ Temporary/Contractual)
3. Faculty (Teaching)
4. Administrative Staff (Non-Technical / Technical)
5. Higher Authorities and Officers
6. Guests.

2.2 Resources

1. Network Devices wired/wireless
2. Internet Access
3. Official Websites, web applications
4. Official Email services
5. Data Storage.
6. Mobile/ Desktop / server computing facility
7. Documentation facility (Printers/Scanners)

3 IT Hardware Installation Policy

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

(i) Primary User:

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be 'primary' user. If a computer has multiple users, none of whom are considered the"primary" user, the department Head should make an arrangement and make a person responsible for compliance.

(ii) End User Computer Systems:

Apart from the client PCs used by the users, the university will consider servers not directly administered by IT Team, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the IT Team, are still considered under this policy as "end users" computers.

(iii) Warranty and Annual Maintenance Contract:

Computers purchased by any Section/Department/Project should preferably upto 3-year on site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include Hardware, Software and related issues.

(iv) Power Connection to Computers and Peripherals:

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

(v) Network Cable Connection:

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

(vi) File and Print Sharing Facilities:

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

(vii) Shifting Computer from One Location to another:

Computer system may be moved from one location to another with prior written intimation to the IT Team Head, as IT Team maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (from the list maintained by IT Team) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs IT Team in writing/by email, connection will be restored.

(viii) Maintenance of Computer Systems provided by the University:

For all the computers that were purchased by the university centrally and distributed by the Engineering Section. The University IT Team will attend the complaints related to any maintenance related problems.

(ix) Noncompliance:

DU faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related

problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effect on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

(x) INTERNET UNIT/COMPUTER CENTER Interface:

INTERNET UNIT upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

4. Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

(i) Operating System and its Updating:

- Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

- University Policy encourages user community to go for open source software such as Linux, Open office, Tools, etc., to be used on their systems wherever possible.

- Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates a being done properly.

(ii) Antivirus Software and its updating:

- Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

- Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

(iii) Backups of Data:

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on Floppy, or CD or other storage devices such as pen drives.

(iv) Noncompliance:

DU faculty, staff, and students not complying with this computer security pol- icy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons An individual's non-compliant computer can have significant, adverse af- fects on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

(v) Internet Unit/Computer Centre Interface:

INTERNET UNIT upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

5. Policies Related to Network Use (Intranet and Internet)

Network connectivity provided through the University, referred to hereafter as "the Net- work", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Communication and Information Services (INTERNET UNIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to INTERNET UNIT.

(i) IP Address Allocation:

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the INTERNET UNIT. Following a systematic

approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorisedly from any other location.

As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the INTERNET UNIT. An IP ad- dress allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

(ii) DHCP and Proxy Configuration by Individual Departments /Sections/ Users:

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by IN- TERNET UNIT.

Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

(iii) Running Network Services on the Servers:

Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server,

only after bringing it to the knowledge of the INTERNET UNIT in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

INTERNET UNIT takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property. INTERNET UNIT will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to anyand all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at INTERNET UNIT. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

(iv) Dial-up/Broadband Connections:

Computer systems that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the university's security by way of bypassing the fire-walls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

(v) Wireless Local Area Networks:

- This policy applies, in its entirety, to Blocks/School, department, or division wireless local area networks. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.
- School, departments, or divisions must inform INTERNET UNIT for the use of radio spectrum, prior to implementation of wireless local area networks.

- School, departments, or divisions must not operate wireless local area net- works with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
- If individual School wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Co-ordinator, INTERNET UNIT.

(vi) Internet Bandwidth obtained by Other Departments:

Internet bandwidth acquired by any Section, department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately e- quipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to INTERNET UNIT. Non-compliance to this policy will be direct violation of the university's IT security policy.

6. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staffs and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic and other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to other area user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources (HR) information, policy messages,

general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to G- Suite (IP:192.168.100.1), with their User ID and Password. For obtaining the university's email account, user may contact IT Team for email account and default password by submitting an application in a prescribed proforma. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

(i) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

(ii) Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

(iii) While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

(iv) User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

(v) User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.

(vi) Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

(vii) User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

(viii) User should refrain from intercepting, or trying to break into others email accounts,

as it is infringing the privacy of other users.

(ix) While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

(x) Impersonating email account of others will be taken as a serious offence under the university IT security policy.

(xi) It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

(xii) Any Spam mail received by the user into Inbox should be forwarded to spam@davangereuniversity.ac.in

(xiii) Any mail wrongly stamped as SPAM mail should be forwarded to wrongspam@davangereuniversity.ac.in

(xiv) All the mails detected as spam mails go into SPAM MAIL folder of the respective user's mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to netadmin@davangereuniversity.ac.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible. The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Gmail.com/Hotmail.com/Yahoo.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

7. Web Site Hosting Policy

(i) Official Pages:

Sections, departments, and Associations of Teachers/Employees/Students may have pages on DU's Intranet Channel of the official Web page. Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting. As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., http://www.davangereuniversity.ac.in only. Personal Pages: The university computer and network infrastructure is a limited resource owned by the university. It is recognized that each individual faculty will have

individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the university by sending a written request to INTERNET UNIT giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the university. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups. Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the university. Affiliated Pages: Faculty may host Web pages for ”affiliated” professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

(ii) Web Pages for eLearning:

Though the university does not have this facility as on this date, this Policy relates to future requirements for Web pages for eLearning authored as a result of Teaching/Learning process. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department’s pages. Because majority of student pages will be published on the University’s Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official DU or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project. The following are the storage and content requirements for class-generated student Web pages:

- Servers: It is recommended that pages be placed on the student information server, but pages developed for classes also may be placed on departmental

servers or the main campus server meant for eLearning purpose.

- Maintenance: If the pages are published on the eLearning information server, they will be maintained under the default rules for personal eLearning pages The instructor will maintain pages that are published on departmental servers or the main campus server meant for eLearning purpose.
- Content Disclaimer: The home page of every class-generated site will include the Davangere University Content Disclaimer (for pages published on the eLearning information server, the content disclaimer should be generated automatically):
- Class Information: The home page of every class-generated site will contain the name of the class, the student's name, the date, and a link to the class home page.
- Pages Generated by Class Groups: Pages produced by class groups, if placed on the eLearning information server, will be placed on the server under the name of the designated group leader.
- Official Pages: If Web pages developed for eLearning become the part of the "official" Davangere University page, they must be removed from the eLearning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

(iii) Student Web Pages:

Though the university does not have this facility as on this date, this policy relates to future requirements for personal student Web pages. Policies for student pages authored as a result of academic assignments are in II above. It is recognized that each individual student will have individual requirements for his/her pages. As the university's computer and network infrastructure is a limited resource owned by the university, only web pages of students related to their assignments will be accepted on the Students web pages. The contents of personal pages hosted by the students even on outside web site must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise

violate any local, state, or central government laws. The following are the storage and content requirements for personal student Webpages:

- Servers: Pages will be placed on the student information server.
- Maintenance: Pages published on the student information server will be maintained under the default rules for personal student pages.
- Content Disclaimer: Every personal page will include the DU Content Disclaimer (the content disclaimer will be generated automatically):
- Responsibilities for Those Maintaining Web Pages: Sections, departments, units, and individuals are responsible for maintaining their own Web pages. Davangere University Webpages (including personal pages) must adhere to the Davangere University WebPage Standards and Design Guidelines and should be approved Davangere University WebPages Advisory Committee.
- Policies for Maintaining Web Pages: Pages must relate to the University's mission. Authors of official DU and affiliated pages (not class-generated or personal) are required to announce their Web presence by sending an announcement to webmaster@davangereuniversity.ac.in. Mails sent to this address will be placed in a DU Public E-Mail Folder in the DU's official web site.

The announcement should include:

- The URL.
- A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the Davangere University Home Page and, if applicable, contain additional links to the sponsoring organization or department.

8. University Database (of eGovernance) Use Policy

This Policy relates to the databases maintained by the university administration under the university's eGovernance. Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. Davangere University has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this universityresource.

(i) Database Ownership:

Davangere University is the data owner of all the University's institutional data generated in the university.

(ii) Custodians of Data:

Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

(iii) Data Administrators:

Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

(iv) MIS Components:

For the purpose of eGovernance, Management Information System requirements of the university may broadly be divided into seven categories. These are:

MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)
FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIM- S)
PROJECT INFORMATION MONITORING SYSTEM (PIMS)
LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYS- TEM (DMIRS)

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.

Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only.

One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies the university makes information and data available based on those responsibilities/rights.

Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the University Registrar.

Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for response.

At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the university or its departments.

All reports for UGC, MHRD, NAAC and other government agencies will be prepared/compiled and submitted by the Registrar, Registrar (Evaluation), Directors, and Finance officer of the University.

Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to;

- Modifying/deleting the data items or software components by using illegal access methods.
- Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers. Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities.

9. Violation, Implementation and Review of the Policy

Any volition of the basic objectives and areas mentioned under the IT policy of the University shall be considered as a violation and as a misconduct and gross misconduct under University Rules.

For implementation of this policy, the University will decide necessary rules from time to time. The policy document (this document) needs to be reviewed at least once in two years and updated if required so as to meet the pace of the advancements in the IT related developments in the industry.

10. Tips and Dos and Don'ts

Do not share your passwords.

Turn off electronic devices (monitors, computers, panels, TVs, projectors and others) when not in use to prolong the life of the devices.

Save all your documents/files to your Hard-drive to avoid losing any kind of data.

When logging into a computer use YOUR user name and password not somebody else's and do not let anybody else use yours.

Do not shut-down systems abnormally.

Usage of external storage should be used on permission.

Any external documented e.g email attachments, pendrives, CD/DVDs should be scanned and used.

Only be logged into one computer at a time, allow others to use it.

Do not install personal softwares in the University systems.

Do not download/open illegal/pirated multimediafiles.

11. Acknowledgements

Davangere University wishes to acknowledge the following Departments/ Institutions/Universities whose related policies and procedures provided background foundation in the preparation of this policy document:

i. Shavaji University, Kolhapur.

ii. Rani Chennamma University, Belgavi.

iii. IQAC, Davangere University.

iv. Department of Computer Science, Davangere University.