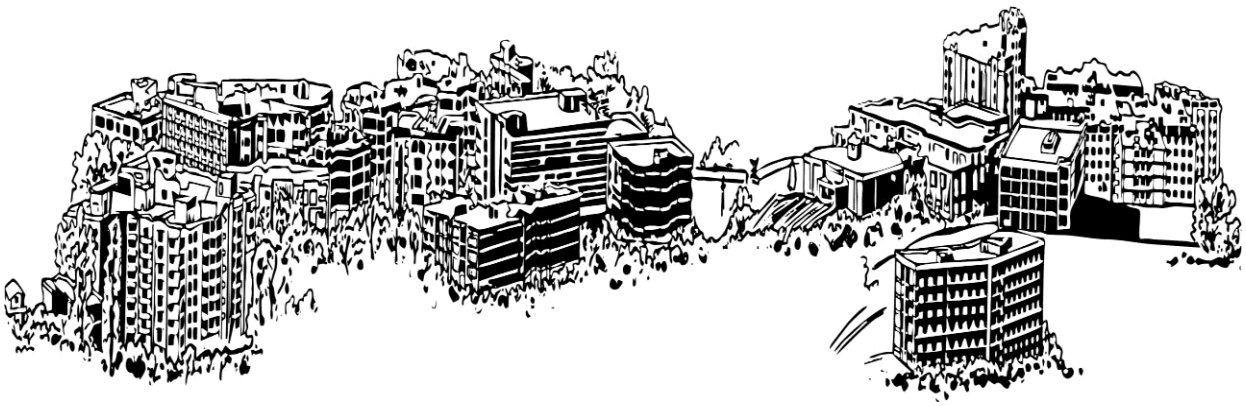
INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

DIT UNIVERSITY

IMAGINE ASPIRE ACHIEVE



Version 2.0

DIT University

Mussoorie Diversion Road Dehradun, Uttarakhand-248009

Information and Communication Technology (ICT) Policy (Version 2.0)

1. Introduction

The DIT University has invested adequately on ICT resources and services since its inception. The amount of computers within the University has now exceeded 1400 desktops, with network facilities. The ICT network includes a fiber optic backbone and a number of STP LANs covering approx. 5000 network connections in more than 12 buildings including academic, administrative and hostel blocks across the campus. This entire network infrastructure is being managed by University Central Server Room under CITM (Center of Information & Technology Management).

2. Rationale

Major considerations for formulating this ICT policy are:

(a) Rapid changes in technologies require proper planning in order to avoid incompatibility and inaccessibility.

(b) Industry 4.0 and the New National Education Policy 2020, warrant a deliberate effort to encourage use of ICT for the Teaching, Learning & Evaluation Processes.

(c) To encourage faculty and staff to be tech savvy and create a pool of adequately trained, system administrator / manager, network administrator / manager and software engineers, coupled with long training constraints ICT developments.

(d) To encourage optimum use of business processes.

(e) To keep pace with the progressive demands of capacity building.

3. Aim

To support the strategic vision of the University by improving operational efficiency, create knowledge repository and exchange of information, so as to retain a competitive edge.

4. Rules for University Computer Facilities Utilization

(a) Access Control

i. Unique IDs of using ICT resources have been assigned to individual from central Server Room of University. Sharing these IDs is prohibited.

ii. No Computers, workstation and laptops should be left in “Logged in” mode as this is antisocial and a security risk too.

iii. **Terminals Usage**: Users are entitled to logout others prior to using a terminal.

(b) Do's

i. All work must be backed up on MS-One drive by individual before leaving computer.
ii. Login password must be changed on periodic basis to avoid any data theft etc.
iii. Ensure to remove your data from C:\ drive on sharing computers.
iv. Report any computer faults to Server Room support desk on ext. 4025.

(c) Don'ts

i. Do not play games on University computers.
ii. Do not consume Food & beverages while working on computer devices.
iii. Do not send personal mail using official mail ID.
iv. Do not indulge in illegal / restricted activity which includes accessing restricted sites e.g. Pornography, Gambling, un-solicited sites, nefarious activity or otherwise not relevant to official work.
v. Do not use hardware / software which may compromise the security of the network infrastructure of University.
vi. Do not move Computer unit without the consent and presence of ICT Representative. This can upset the cabling, potentially compromising the network or preventing a workstation from operating.
vii. Do not change computer hardware / network settings without the consent of ICT officials.

5. Rules for Network Use

(a) Ethernet socket is solely used for computer connection using Ethernet cable. Do not connect any other device.
(b) Only one Ethernet card is to be configured in a computer, no additional Ethernet card installation is allowed.
(c) Use of Personal network devices is prohibited in the University network which includes Wi-Fi hubs / switches, etc.
(d) Faculty and staff members are not allowed to install any unauthorized software's in computers, including in LABs and official computer / laptops.
(e) Software's are to be installed in computers and laptops by Central Server Room team after approval of Department head and consent of the authority.
(f) Access to University network is with proper authentication, unauthorized persons are not allowed to access University network, thus, do not share log in credentials.
(g) Network uses authentication in form of unique staff ID. This is provided to University staff members from Server Room after approval of HR Department.
(h) E-mail IDs will be provided from Server Room to University staff after approval from HR Department.

6. IT Hardware Installation Policy

All stakeholders (Schools, Departments, Central Facilities, Laboratories, and Individuals) who have been allotted IT Hardware in their domain of functioning must:-

(a) Connect their systems (computers and peripherals) to authorized UPS electrical power outlets to avoid system damage.

(b) All Heads to ensure that every IT equipment in their domain of functioning is under the ownership of designated employee. Thus, the department must identify the end-users.

(c) Computer systems, if any, either in lab or with individual, which is used as servers and created only for Teaching and Learning purpose are considered under this policy as "end users" computers. These will not interfere with the services of CITM.

(d) All the systems installed at user end or in labs are of latest configurations and purchased by a reputed manufacturer of IT industry. HP and IBM are two branded suppliers of systems, laptops and servers in the University.

(e) After the expiry of warranty, computer maintenance is handled by the ICT technical staff of DIT University and the servers are given under annual maintenance contract.

(f) Any requirement of shifting of computer systems from one location to another should be with prior written intimation to the ICT Manager Server Room, and with proper approval of concerned authority.

(g) All IT Hardware should be properly tagged, which denotes belonging departments and areas.

7. Software Installation and Licensing Policy

(a) Pirated / unauthorized software is prohibited on Campus. Do not install unauthorized software in any computers/ laptops which is networked on campus in the University. The University ICT Policy strictly endorses the Anti-piracy Regulation of GoI.

(b) Software including operating system, office suite antivirus and necessary standard applications will be provided by CITM Dept. (Server Room).

(c) Any additional Software requirement of the department or departments should be routed through proper justifications and approvals of concerned authority. Verification by CITM prior to procurement process should be initiated.

(d) DIT University labs as well as individuals are required to use Licensed / Genuine software and applications. In case of any discrepancies in operating system and software installation, ICT officials should be intimated about the problems.

8. Network (Intranet & Internet)

(a) Network Resources

The IT infrastructure for DIT University consists of high end wireless and wired devices. Access points of leading brands in the field of networks are installed in all the Hostels.

Presence of Sophos and D-Link ensures appropriate and reliable wireless access points for higher-class enterprise environments. Designed for indoor installation, this access point provides secure options for network administrators to deploy a highly manageable and extremely robust wireless network. These access points support Power over Ethernet (PoE) and provide two high-gain antennas for optimal wireless coverage.

Apart from wireless connection, Internet connection is also available through wired connections. High-quality Gigabit, Ethernet ports are installed in the buildings, providing wired Internet access through a copper cable.

High-speed fiber-optic backbone is connected to the internal network through a high-end gigabit Ethernet switch.

(b) Wireless Networks

Server Room ICT Team is authorized to consider the applications of departments, or divisions for the use of radio spectrum. In case access through Fiber Optic/UTP cables is not feasible, in some locations, Server Room ICT Team considers providing network connection through wireless connectivity.

(c) Internet Resource Optimization

Internet is being provided through high-speed fiber-optic backbone of overall bandwidth of 1489 Mbps from reputed ISPs including Vodafone, etc. Further the INTERNET is provided through our internal gateway i.e., our UTM device Sophos XG550 and IP distribution by DHCP server.

DHCP server provides IP addresses to the users connected to the network through the wired as well as wireless device installed in the campus.

For smooth functioning and to maintain high levels of security, the University adheres to specific protocols. Thus, allocation of unique IP address, based on location / department facilities timely troubleshooting and security breaches, encryption, password protection and mandatory access login have been implemented to ensure “Closed domain” configurations.

9. Email Account Use Policy

E-mail service ID is provided to University staff for formal mail communications by the approval of HR department. This facilitates the delivery of messages and documents to University staff as well as

external communications. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

(a) All employees and Students must use the allotted / allocated email id for all official correspondence.

(b) The facility should be used primarily for academic and official purposes.

(c) User should avoid sending large attachments. If necessary, use “One Drive” to send the same and ensure recipient can access it.

(d) All mail users should follow the 80% mailbox usage threshold, to avoid any mail bouncing.

(e) Mail users must not open suspicious mail and attachment from unknown sources, these types of attachments can damage your computer and data.

(f) All mail users should configure messaging software (Microsoft Outlook,) on the computer to access mail service. This is required to keep local mail backup and reduce server space.

(g) E-mail users are solely responsible for their e-mail IDs. Do not share the email.

(h) Logout of the official computers after every email session, to avoid misuse on shared computers.

10. Electronic logs

All network traffic logs are created in system as a monitoring process. These logs are kept for ICT administrative need and are destroyed periodically and timely.

11. Global Naming & IP Addressing

Server Room ICT Team is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. Server Room monitors the network to ensure that such services are used properly, Providing Net Access IDs and email Accounts.

Server Room ICT Team provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the University upon receiving the requests from the HR Department.

12. Network Operation Center

Server Room ICT Team is responsible for the ICT operation of the centralized Network distribution from central Server Room. This network includes Internet facility provided 24x7 on-campus. Any network failure and issues are to be reported to Server Room. The ICT support team will resolve the issues.

13. Backup & Archival Policy:

(a) Central Network: Centralized backup is a process of sending required data to remote sites for storage. This process takes immense use of network bandwidth, but it provides data at the time of natural calamity at parent location.

University CITM Department is to arrange for NAS drive / appropriate contemporary technological tools to cater for system and data backup at remote location. However, this data consumes time and Internet bandwidth but provides data availability if required in worst conditions. To address these concerns, CITM administrator should configure backup strategy in a manner to send only incremental data backup.

(b) ERP: University implemented SAP as an ERP solution. This solution requires strong backup strategy. SAP Servers backup enables to recover a damaged database. A well-designed backup and restore strategy maximizes data availability, minimizes data loss resulting in minimum downtime. All server backups are taken as per below strategy.

Server Name	Backup Strategies	Backup Retention Period
ERPDITECD	Daily Transaction Log Backup, weekly DB Backup and Monthly Image Backup of OS.	Two Successful Backup and all T- Log Backup
ERPDITECQ	Daily Transaction Log Backup, weekly DB Backup and Monthly Image Backup of OS.	Two Successful Backup and all T- Log Backup
ERPDITECP/ DBP	Hourly Transactional Backup, Daily DB Backup and Monthly Image Backup of OS.	15 Successful Backup and all T-Log Backup
EPDITEPD	Daily Transaction Log Backup and weekly DB Backup	Two Successful Backup and all T-Log Backup
EPDITEPO	Daily Transaction Log Backup and weekly DB Backup	Two Successful Backup and all T-Log Backup
EPDITEPP	Hourly Transactional Backup, Daily DB Backup and Monthly Image Backup of OS.	10 Successful Backup and all T-Log Backup
DMSDITSCD	Daily Transaction Log Backup, weekly DB Backup, Monthly File system Backup and Monthly Image Backup of OS.	Two Successful Backup and File system Backup
DMSDITSCP	Daily DB Backup and Monthly File System Backup and Monthly Image	7 Successful Backup and all T-Log Backup

Server Name	Backup Strategies	Backup Retention Period
	Backup of OS.	
SOLMANDITD	Monthly DB Backup	Two Successful Backup and all T-Log Backup
Web Dispatcher	Monthly OS level Backup	Two Successful Backup and all T-Log Backup

(c) Individual Computer System Data: It is one of "Users" most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. This paragraph amplifies the process to backup & restore data residing on University desktop computers and laptops.

"User data, especially work-in-progress, should be saved to a local computer drive and then that must be backed up every day or weekly onto storage media such as "One Drive" Online with 1 TB storage capacity already provided by the University to every individual user."

14. Disaster Management & Computer Emergency Response Team (CERT):

To cater to disaster management, CITM must use specific mitigation measures to overcome disaster such as Clustering physical servers, storage RAID technologies, power redundancy of servers including storage and switches / routers and any other contemporary technological solutions. This will ensure Disaster Recovery which is a combination of data backup and disaster recovery solutions that work cohesively to ensure University digital process continuity. Under this DR (Disaster Recovery), prevailing methodology is remote data backup placed at remote locations securely. This enables to recover data at the time of any natural disaster.

15. Inventory Control & Stock Receipt / Issue / Renewal.

The inventory is usually issued from the University's central inventory as and when it is required. "Issue/ Receipt" refers to the transactions, between the CITM & end user, related to IT equipment (Hardware/ Software) procured and utilized under the budgetary heads allocated. Accordingly, the stock register is updated and periodical renewal of issue vouchers is undertaken (on exit / entry of employees/ students and annually as the need arises).

16. Equipment obsolescence and upgradation:

The Information and Communication technology (ICT) has provided many facilities in a way to organize our lives. In this context, rapid technological advancement has resulted in manifold generation of obsolete equipment and hazardous waste. This

waste may put wrong impact to human health and environment. Addressing the correct disposal of hazardous E-Waste is therefore critical.

University centrally consolidates the disposal of all such types of e-waste. CITM is the custodian of IT (HW&SW) and is responsible for collating the details from divergent departments which is declared as e-waste. This will subsequently be disposed of as per Govt. regulations through the Administration wing of the University.

17. Force Majeure & VUCA Environment

Conditions and circumstances beyond the control do require innovative and creative solutions. The Volatile, Uncertain, Complex & Ambiguous situation we are currently confronting warrants the flexibility and adaptations. Issues related to "Online" Teaching Learning and Evaluations will be reviewed regularly and SoPs will be issued for compliance based on the Operational, Technological Advancements & Regulatory stipulations.

18. Free and Open Source Software Policy Initiatives

Directives of MHRD mandate that online learning resources must include free and open source software in education (FOSSE). DIT University promotes and facilitates the use of open source software in education for teaching learning processes. SoPs, Webinars and Seminars associated with such activities are to be shared and faculty members are encouraged to participate actively. In this connection, the University has constituted Center of Online and Remote Learning (CoREL), which would periodically be the facilitator for utilizing the GoI and MHRD initiatives such as:-

SWAYAM	National Digital Library (NDL)	e-Yantra
SWAYAMPRABHA	FOSSEE (R, Python Moodle etc.)	DIKSHA
Virtual Labs	Gyan Vani	e-PG Pathshala
e-gyankosh	e-ShodhSindhu	Shodhganga
Gyan Darshan	Shodh Shudhhi	VIDWAN
Spoken Tutorial	NEAT	SAKSHAT

These initiatives will improve the quality of Teaching & Learning and Research capability, thus, enabling the institution to increase its visibility and in perception management.

19. Compliance & Violations

It is mandatory for all Staff / Faculty members/ Students to adhere to the specifics mentioned in this Policy document. In addition, attention is drawn to all stakeholders to adhere to the Government of India Laws related to GoI IT ACT 2002 & Cyber Security stipulations of the Regulators

(a) Any breach of University ICT rules, the use of Ethernet socket and Wi-Fi will be

suspended until the matter is resolved.

(b) **All violations and compromises by stakeholders will be dealt with as per the DIT University Service & Conduct Ordinance for Employees and Students.**

(c) **In case of any dispute, the decision of the Chair of the ICT Committee will be final.**

20. Conclusion

As a concluding note, it is explicitly emphasized that though the policies focus on issues related to the technology and information usage. It may be understood that they derive broader meaning and significance from not only fundamental rights but also basic rules and responsibilities that apply to all aspects of the University community. If something is not specified explicitly in the policy or guidelines as illegal or unauthorized, it may still be in traction of the University rules, if it violates the basic rules and responsibilities of the University. So, it is essential and important to use one's own wisdom and critical thinking in evaluating new situations.

*****