SHRI GURU RAM RAI UNIVERSITY
Quest for Excellence

# I C T Policy

SHRI GURU RAM RAI
UNIVERSITY
*Quest for excellence*

# ICT POLICY



## SGRR University, Dehradun


# CONTENTS OF ICT POLICY

## 1. PREAMBLE:

The rapidly increasing usage of information and communication technologies is a welcome change in recent years. ICT increases productivity, improves the working life of employees, and provides better opportunities for school management, employees, and students. Today, ICT plays a key role in the development of processes, thereby increasing the quality and efficiency of human work.

**The policy addresses the five essential components of ICT as outlined below:**

ICT infrastructure , Education, the work of ICT and other non-IT people, Improving Information and Communication Technology and overall Productivity and monitoring this law, once formed and implemented, contemplates continuing monitoring, periodic inspections, and fines based on enforcement and performance.

Shri Guru Ram Rai University (SGRRU) offers various programs in 11 schools. SGRRU ICT Policy is used in Arts, Sciences, Business, Medicine, Management, Nursing, Paramedical & Health Sciences etc. It offers Certificate, UG, PG, Diploma and Doctorate programs in different fields. It aims to provide access to ICT services by students, staff, management, and all stakeholders. The objective is to contribute in the development of the society by transforming the university into a digital and paperless university that can be accessed anytime and anywhere.

## 2. WHAT IS ICT?

"ICT" refers to Information and Communication Technology and all forms of communication, such as the Internet, wireless networks, mobile phones, computers, software, video conferencing, social networking, and other media applications and services used to access, store, modify, and manage data and information.

When faculty members are technologically knowledgeable and understand how to incorporate ICT into their curriculum, it has a positive impact on students' learning. Schools use a variety of ICT tools like smart boards, LCD projectors, LAN, Wi-Fi, and software tools like google classrooms, google sheets etc. to transmit, create, publish, store, and manage data and information.

## 3. ICT AT SGRR UNIVERSITY

In addition to traditional teaching, teachers also use knowledge-based learning tools and e contents such as PPT, videos, online classes, online resources to enable students to gain knowledge and academic success. In SGRR University classrooms and seminar halls are well equipped with ICT facilities. University is having adequate number of seminar halls and classrooms with ICT enabled facilities such as:

1. Smart Board
2. LCD projectors
3. LAN (Local Area Network)
4. Wi-Fi

## 4. ICT INFRASTRUCTURE

ICT infrastructure mainly includes hardware, systems, and application software. It also comprises of wired and wireless communication infrastructure such as cables and network equipment for internal and external communication.

### 4.1 ICT HARDWARE

Hardware comprises of various products used by end users as well as gadgets that assists the end users in using ICT such as servers, desktops, laptops, tablets, smart-phones. Hardware accessories include printers, scanners, UPS, network switches, bridges, routers, brouters, gateways and so on.

### 4.2 ICT SOFTWARE

System software is software that makes the system work and is an essential component of the system.

An operating system is an example of system software whereas E-mail clients is an example of application software. System Software is either proprietary, like as Windows, or open source, such as Linux. Application software, such as Microsoft Office and Outlook, is proprietary. Open-Source software includes Thunderbird E-Mail, Open Office Suite, and more.

Users usually opt for open source software as it is available for free or at a reduced price. To maintain format uniformity and simplicity of information exchange across the University, software should be employed.

### 4.3 ICT COMMUNICATIONS INFRASTRUCTURE

Covers both wired and wireless ICT-based communications within and beyond the University. Cables, Junction Boxes, Switches, Modems, Bridge, Routers, Brouters, Access Points, Gateways and other networking equipment's are also included.

## 5. ICT PROCUREMENT MAINTENANCE AND UPGRADATION POLICY

### 5.1 ICT PROCUREMENT POLICY

a. The ICT Infrastructure Management Committee (IIM Committee) is responsible for defining, reviewing, updating, approving, and publishing the web/annual ICT infrastructure management policy.
b. All users must abide by the rules set by the ICT Infrastructure Management Committee.

c. All users must get prior permission from IIM Committee for the requirements and specifications of the ICT equipment they need.

d. IIM committee must meet in the start of semester and end of semester

e. The Committee shall work to standardize the terms and conditions as well as the purchase procedures for ICT equipment and software in accordance with national and central government ICT policies and guidelines.

f. The procurement process must comply with the University Grants Council, state and central government accounting and auditing policies and guidelines.

g. Bulk purchases, along with the need for similar equipment, should encourage the best deals. Original equipment manufacturers (OEM) suppliers should be preferred for hardware as well as software. Special Price for Educational University to be taken from major brands like IBM, HP, DELL. For networking only top brand CISCO must be used.

h. Electrical Wiring should be branded such as Havells or Polycab. Local wires will not be used. Wiring must be Fire Proof to prevent incidences of fire in computer laboratory

**Within the scope of the ICT procurement policy, the following points should be considered:**

**Feasibility:** If the project and technology is not yet available and is being introduced, a design suitable for the introduction of the new project and technology should be prepared in advance. It should also take into account alternative technologies as well as the reason behind selecting the particular technology. Preference will be given to the latest technology introduced in the market.

**Cost Benefit:** The initiator of the proposal must provide a statement outlining the cost versus projected benefit of the purchase. If the result is subjective, the assessment based on the basic structure and a 1 to 10 ranking should be submitted. This will help providers match needs with available technology.

**Planning and budgeting:** All universities and departments should plan ahead of time for their ICT demands and include them in their budgets. The budget should pay for capital investment as well as operating expenses. This will help manage cash flow while developing ICT resources.
Specifications and configurations available for purchase must comply with usage plans and the Information Technology (ICT) Act SGRRU, created in consultation with members of the ICT Infrastructure Steering Council.

**Financing:** Appropriate financing should be provided for the purchase of ICT. The University's financial professionals can advise on other ways to finance the ICT resources purchase, as appropriate. It is also necessary to have a pool so that it can replenish the budget when purchasing quality falls below the budget.

**Accounting:** All ICT infrastructure, including hardware, software, networking and communication equipment, has costs that must be properly accounted for. These items should be considered as assets and their acquisition, transfer and disposal should always be reflected in the asset books.

**Insurance:** ICT insurance is required and all products must be covered by a general insurance policy or - for specialty products - an electrical specific policy.
For example, servers must be covered by electronic rights with data recovery capabilities. Insurance against data loss and recovery costs should also be considered.

**System Audit:** Inspection and physical analysis of ICT assets should be done to ensure that all assets are up to date, working as expected, and are suitable and not normal. This type of analysis helps to identify in advance which items needs to be replaced in a timely manner so that they can be well prepared. This study will prevent the reduction of the workload of ICT services.

**Information security:** Data security has many features. They are separated into digital and physical. Security related to digital devices is related to passwords, access rights, backups, anti-virus measures, external media etc.

Physical security includes controlling access to physical space, preventing unauthorized personnel, providing electrical and fire equipment, monitoring with CCTV cameras, etc. On the other hand, physical security includes distribution, storage and maintenance of information, controlling access to confidential information and scheduling for secure maintenance, sharing confidential information, inadvertent leakage of classified information etc.

**Outsourcing:** Outsourcing is very useful and inevitable in today's world, but there are many things to consider when outsourcing or hiring outsiders in university. These concerns may include providing outside business information, completing certain repairs, disposing of products/equipment, etc. includes - all of which should be carefully considered regarding ICT safety and security. Similar precautions should be taken when completing a turnkey project using ICT.

**Best Practices:** Employees should be appointed to keep up with technological developments and should be appointed to determine the procedures necessary for the new/goods of technology to be used for profit. They should also educate themselves on best practices recommended and/or followed elsewhere that will benefit the university.

**5.2 ICT MAINTENANCE & UPGRADATION POLICY**

**a.** On procurement & installation of any new ICT device/equipment, User department must allocate a unique dead-stock number (Asset Identification Number) in the dead stock/Asset Register. The same number must be written on the front side of the device/equipment, which can be used for physical verification. The same must be appropriately updated while transferring out OR disposing/writing off such assets.

**b.** User department must be vigilant about warranty checks and must take appropriate action if the performance of the device/equipment deviates from the expected performance.

**c.** After the completion of the warranty period, User Department may implement the Annual Maintenance Contract (AMC) for the device/equipment depending on the criticality of its usage, with the approval of the ICT Infrastructure and Management

Committee & following the standard procedure laid down by the university from time to time.

**d.** The ICT Infrastructure and Management committee shall define, review, revise, approve and circulate/publish the guidelines & procedure for up-gradation of outdated ICT devices/equipment's/components or to improve the performance of existing ICT devices/equipment's/components and software. The upgradation of devices/equipment can be through increasing the performance capacity by adding/replacing some components, like memory, HDD, Graphic card etc. or by replacing the whole device/equipment through a buy-back mechanism depending on the specifications and performance parameters of the device/equipment. Prior approval of specifications and requirements by the IIM Committee is essential.

**e.** Necessary budget provisions must be made by the respective user departments for the maintenance and upgradation of its ICT equipment hardware and software.

## 6. ICT POLICY FOR WRITING-OFF ICT EQUIPMENT

ICT Infrastructure Management Committee (IIM Committee) is responsible to define, review, revise, approve and circulate/publish the guidelines & procedure to scrap and write off the non-functional, non-operable, non-repairable and obsolete ICT devices/equipment's. It must perform the vendor evaluation and registration process to identify & register the vendors specialized in disposal of e-scrap or digital scrap.

## 7. ICT USAGE POLICY

### 7.1 ICT ETHICAL USAGE GUIDELINES

a. All users should use the ICT resources they access in an understandable and conscious manner.

b. Intranet and Internet access may not be used for commercial, personal advertising,

solicitation, or promotion, such as hosting or linking to commercial websites or email broadcasts of commercial promotions to the users

c. No part/content of the University's ICT infrastructure may be misused for anti-university, anti-government or anti-national purposes.

d. The ICT Policy Committee will be authorized to take the necessary measures to maintain these disciplines in order to prevent undesirable activities.

e. Non-MSU organizations (such as commercial outlets operating on the MSU campus, IGNOU, USET etc.) will not be connected to the MSU-Intranet, and cannot be a part of the MSU domain space.

f. Downloading audio and video files should be done strictly for official purposes.

g. All users must preserve and maintain the confidentiality of the passwords they use. No user may knowingly or accidentally try to use another user's password to access ICT resources.

h. Access to websites that are prohibited by law or that are offensive or obscene is prohibited.

i. This is also a crime and is punishable by severe penalties.

j. Use of the network to interact with other computers' data, hack the computer and taking information from that computer, distribution, interfere with other systems or use the Intranet/Internet to cause any kind of harm is prohibited and illegal.

k. In addition to the violation of laws under the IT Act 2000, the user is also liable for material damages under this law.

l. No device/user other than those registered with the university can be used to connect to the intranet.

**7.2 ICT GUIDELINES FOR USERS AS PER THE INFORMATION TECHNOLOGY ACT, 2000**

a. To tamper with the source documents of computer system will lead to imprisonment up to three years, or/and with fine up to ₹200,000

b. To hack computer system and use of password of others will lead to imprisonment up to three years, or/and with fine up to ₹500,000
c. To receive or purchase stolen communication device or computer system will lead to imprisonment up to three years, or/and with fine up to ₹100,000
d. To use password of another person will lead to imprisonment up to three years, or/and with fine up to ₹100,000
e. To do cheating using computer or ICT resource will lead to imprisonment up to three years, or/and with fine up to ₹100,000
f. To publish private images of others will lead to imprisonment up to three years, or/and with fine up to ₹200,000
g. To do act of cyber terrorism will lead to imprisonment up to life.
h. To publish child porn or predating children online and publication of information which is obscene in electronic form will lead to imprisonment up to five years, or/and with fine up to ₹1,000,000
i. To publish images containing sexual acts will lead to imprisonment up to seven years, or/and with fine up to ₹1,000,000
j. To secure access or attempt of securing access to a protected computer system will lead to imprisonment up to ten years, or/and with fine.
k. To misrepresent the facts will lead to imprisonment up to 2 years, or/and with fine up to ₹100,000
l. To breach privacy and confidentiality will lead to Imprisonment up to 2 years, or/and with fine up to ₹100,000
m. To disclose information to others in breach of lawful contract will lead to Imprisonment up to 3 years, or/and with fine up to ₹500,000
n. To publish electronic signature certificate false in certain particulars will lead to Imprisonment up to 2 years, or/and with fine up to ₹100,000

o. To publish for fraudulent purpose will lead to Imprisonment up to 2 years, or/and with fine up to ₹100,000

**7.3 ICT CENTRALIZED AUTHENTICATION OF USERS**

a. The Computing Center is responsible for establishing registration and access rights management systems for all users using LDAP or Active Directory or other appropriate software. It should provide a GUI-based platform for user administration where user departments can manage their users in the master database of users in LDAP or Active Directory.

b. The head of each user department is responsible for adding/updating information about their users and access rights to the user database managed by the computer center.

c. The administrator may appoint an employee, preferably a permanent employee, to assist him in managing the information of his users in the central user database and to report to the computer center.

d. With the guidance and support of Information Policy Management, the IT Center will provide all heads and designated employees with the necessary training for managing user information of their respective user department.

e. The user department shall update information of its students after finalization of admissions once every year. The modification of user data for teaching/non-teaching staff and any other user must be updated immediately by the user department with the change in the user status. Individual user is not responsible for updating of his/her information in the user database.

f. The ICT Policy Implementation Committee shall have an authority to override such permissions granted in case of any user.

**7.4 ICT INTERNET & INTRANET APPLICATION SOFTWARE USAGE ONLY BY REGISTERED USERS**

a. Registered users will be allowed to access the Internet and download audio and video, subject to their access rights.

b. Users with selected privileges are granted access to the University's intranet application. For example, responsibility for adding/changing/deleting impact information in student life management software is given only to the University's Education and Research Department staff and teachers.

c. Every Application Software deployed in the university, whether developed in-house or through outsourcing or readymade or cloud based, shall have one administrator user designated by the university. It is the responsibility of the administrator user to manage user access rights. However, non-IT administrators must take guidance and assistance of the Computer Centre in resolving technical issues of the software.

d. Access of non-academic websites, download of music/movies and non-academic videos etc. must be restricted to all users.

e. Faster access to electronic journals registered by UGC-Infonet, INDEST and other educational institutions, the National Digital Library and other projects should be provided.

**7.5 ICT SHARING OF HARDWARE BY EMPLOYEES & STUDENTS**

a. ICT sharing of hardware resources like Desktops, Printers, Scanners by employees and students

b. ICT resources are limited, but there are many users. Therefore, resources need to be allocated effectively and efficiently.

c. Use of network Office equipment like Network Printers and Network Scanners should be encouraged.

d. A minimum computer student ratio of 1:2 is recommended for all IT

programs/courses, and a computer student ratio of 1:4 is recommended for non-IT programs/courses.

e. All schools should maintain a computer staff ratio of 1:2 at best. All other non-teaching/administrative department and offices should maintain a good 1:4 ratio of computer staff.

f. Due care should be taken not to overwrite/delete other users' data on shared resources.

g. Guidance and support is available at the Computer Centre in case of any problem.

### 7.6 ICT UNDERTAKING FOR FAIR USAGE BY ALL REGISTERED USERS

Please go through the following ICT Usage Policy of the **Shri Guru Ram Rai University, Dehradun** CAREFULLY before accepting/rejecting the policy.

**Shri Guru Ram Rai University, Dehradun**

**Undertaking with respect to the ICT Usage Policy**

**Whom this Document Concerns**

All Users of ICT infrastructure (Computers and the Network) at **Shri Guru Ram Rai University, Dehradun.**

**Reason for Policy:**

This policy outlines the responsible use of the Information & Communication Technology Infrastructure at **Shri Guru Ram Rai University, Dehradun.**

**Statement of Policy:**

All users of the ICT facilities of **Shri Guru Ram Rai University, Dehradun** will be subject to the following Acceptable Use of Policy

a. I will be responsible for all use of this network. If I have a computer and decide to connect to the SGRRU network, I am responsible for all content on the computer, especially the content I make available to other users (This provision will also apply to any computer or device for which I am responsible and is included in the meaning of “my computer”).
b. In case I do not own a computer but I am provided some ICT resources by SGRRU, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Centre or Department machines).
c. I will be responsible for all internet traffic generated by "My Computer". I understand that network capacity is a limited resource. I agree that physically tampering with network connections/equipment sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Violation of such rules may result in permanent interruption of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.
d. I understand that the ICT infrastructure at SGRRU is for academic use and I shall not use it for any commercial purpose or to host data/network services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per provisions of Indian law.
e. I will not try to deceive others about myself in electronic or network communications. I will also not use SGRRU ICT resources to threaten, intimidate, or harass others.
f. I will not intrude on the privacy of anyone. I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

g. I understand that the ICT resources provided to me are subject to monitoring, with cause, as determined through consultation with the SGRRU administration, when applicable.

h. The monitoring may include aggregate bandwidth usage to effectively manage limited ICT resources and monitoring traffic content in response to a legal or law enforcement request.

i. I authorize SGRRU administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of SGRRU network.

j. I shall maintain my computer on this network with current Antivirus/Internet Security/Endpoint Protection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, bots, malware and other similar programs.

k. I shall not use the ICT infrastructure to engage in any form of illegal file/data sharing (examples: copyrighted material, obscene material).

l. I understand that I will not take any steps that endanger the physical or logical security of the SGRRU network. I will not specifically try to bypass firewalls. This includes not setting up servers/communication devices (including wireless) of any kind (examples: web, mail, proxy, router, managed or unmanaged switch, smart phones) that are visible to the world outside the SGRRU campus.

m. In critical situations, SGRRU authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of SGRRU. Information & Communication Technology (ICT) Policy SGRRU

n. I understand that any use of ICT infrastructure at SGRRU that constitutes a violation of SGRRU Regulations or provisions of Information Technology Act 2000 could result in administrative or disciplinary or legal procedures.

**8. ICT HARDWARE INSTALLATION POLICY**

The College network client local area needs to notice specific safeguards while getting their PCs or peripherals introduced with the goal that he/she might confront least burden due to interference of administrations because of equipment disappointments.

**9. ICT NETWORKING AND CONNECTIVITY**

Network Connections must be kept away while connecting the PC to the enterprise. It must be kept away from any electrical or electronic device. This impedes the organization correspondence. No other electrical & electronic gadget ought to be imparted to the power supply from where the PC and its peripherals are associated.

**10. ICT MONITORING AND EVALUATION**

1) Computer Center or another employee organization (IA) will have the privilege to review the organization and framework from the common position for this method according to regulations.

2) The IA / Nodal Officer may access, search, print or delete electronic correspondence implied by the University to customers or information stored on gadgets, for security reasons or to comply with applicable legislation. This includes documents, messages, electronic media, website history and more.

3) IA can review the user's internet usage in the University organization according to the working process of the goals & standards.

**11. ICT POLICY REVIEW**

The University reserves the right to change the terms of this regulation at any time. Any such changes will be recorded in the system's revision history, accessible on the SGRRU

website and proceeding to utilize the College's IT Assets following any update it is viewed as acknowledged on the overhauled conditions of this Strategy.

Quest for Excellence”

# SHRI GURU RAM RAI UNIVERSITY

**(Established By Govt. of Uttarakhand, vide Shri Guru Ram Rai University, Act no. 3 of 2017)**