4.3.1

https://hnbgu.ac.in/computer-center

Information and CommunicationTechnology (ICT) (Usage) Policy

Hemvati Nandan Bahuguna Garhwal University

Srinagar (Garhwal)-246174, Uttarakhand, India

Information and Communication Technology (ICT)

(Usage) Policy

Hemvati Nandan Bahuguna Garhwal University, Srinagar (Garhwal)- 246174, Uttarakhand, India

This policy is the guidelines for appropriate use of all information and communication technology (ICT) enabled resources (but not limited to) such as computers, networks, and the information contained therein.

Authority: Approved by the competent authority of HNB Garhwal University, Srinagar (Garhwal) - 246174, Uttarakhand, India.

Applicability: This policy is applicable to all the students, faculty members, staff of HNBGU, guests and all others who use university's Information and Communication Technology (ICT) resources (i.e., all the computers, communication nodes, information and communication technologies (ICT), etc.), within the university's network and access, transmit or store university's and/ or personal information.

Policy Statement: All such aforesaid users SHALL be required to sign an undertaking placed as Annexure – I, at the end of this document. ICT resources of the university should be used to augment various objectives of teaching, learning and research. It is the responsibility of the Users of HNBGU network and computer resources ("users") to appropriately use and protect University's ICT resources and to respect the rights of others. This policy is a guidelines for safer and legitimate use of such ICT resources.

1. **Definitions:**

Terminology as used in this policy:

1.1. "Information and Communication Technology (ICT) Resources" : This includes all the devices and technologies provided by the university, which access, process, store or transmit University's or an individual's personal information.

1.2. "Information" includes both University's and an individual's personal information, both in public or personal domain.

1.3. "Individually owned resources" are ICT resources that are purchased and owned by individuals and are being used within University's prerogatives.

2. Policy:

2.1. General Policy

The University recommends its Users to safeguard

a) The integrity of ICT resources,
b) The privacy of electronic information, and
c) Their own online identity from use by another individual.

User should not attempt to retrieve or gain unauthorized access to any other user's accounts and their ICT resources. Users should safeguard the rights and privileges of owners and publishers over all copyrighted materials, licenses and on other information resources, no matter whether claimed or not.

2.2. Access to ICT Resources

The University prohibits its users from gaining or enabling unauthorized access to forbidden ICT resource on the University's network. Any such attempt will not only be the violation of University Policy but may also violate national and international cyber laws, provisions under the Information Technology Act of India and infringe the principles of National Cyber Security Policy, and subject the user to both civil and criminal liability. However, the University reserves all the rights to access and analyze the ICT resource and Information for any legal and/ or University's provisioned operation, on its own or through its affiliates.

2.2.1. Non-transferable Identities: All user identities on the University network are non-transferable and shall not be shared or used by any other user. Any such known or unknown usage shall constitute violation of the University policy.

2.2.2. Proprietary nature of information: All the information belonging to other users (such as data, programs or any other digital material, passwords, etc.) shall remain proprietary in nature and without obtaining specific permission(s) form respective users, other users shall not use or possess or share any such information in its original or modified form.

2.2.3. Legitimate Use of ICT resources: The users of ICT infrastructure of the University are also by default governed by the prevailing laws of the India. Further, current policy document broadly indicates University's commitment towards observing such security mandates and legal bindings. The 'users' are therefore also advised to be aware

and remain compliant to various legal obligations, licenses, contracts and prevailing Information Technology Act of India, National Cyber Security Policy, etc.

2.3. Prohibited Uses

2.3.1. Prohibited Use: The University prohibits its users from sending, viewing or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material(s) that are a violation of applicable law or University policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful, e.g., when such content is received through e-mail, etc. As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

2.3.2. Caution regarding Copyrights and Licenses: Users must not violate various Intellectual Property Right (IPR) and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file sharing, use of any form of illegal or pirated or un-licensed software, on the University's ICT resources (including individually owned ICT resource being used under University's ICT privileges) is strictly prohibited and any such act shall constitute a violation of the University policy. University also recommends to its students, faculty and office staff, to use Open Source Operating Systems (OS) and Processing Software (PS) such as Ubuntu/ CentOS or other and Libre Office/ OpenOffice/ WPS Office, respectively. Further, users of the computers sponsored directly or indirectly by University should migrate on the recommended OS & PS as their primary software and should generate expertise on it. In case of technical limitation in such adaptation, relaxation may be requested from competent authority on valid grounds.

2.3.3. Terms of Use of Social Media: By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, applications, mailing lists, chat rooms, blogs, etc.

2.3.4. Personal Use: The University's ICT resources should not be used for activities that are unconnected with University's prerogatives towards research and academic functions, except when there is urgency to check personal e-mails, bank and other social accounts, news, etc.

2.3.5. Commercial Use: The University prohibits use of its ICT resources for any commercial purpose except when permitted by appropriate authority. Further, when any such use is permitted, it should be properly related to University activities, and after taking into account all additional liabilities, as may accrue by reason of such activity.

2.3.6. Access to and use of ICT Resource/ Data: The University may generate huge data containing variety of information. For conducting any study or analysis on such ICT resource, prior approval from competent authority MUST be obtained and users must abide by the terms and conditions of grant of such approvals, applicable privacy and other policies.

2.4. Use of individually Owned ICT Resources:

The University does not require or recommend use of individually owned ICT resources to conduct University's tasks. However, individual units may allow its users to use such ICT

resource within the unit only and any such user may choose to use his/her own ICT resources and abide by respective terms and conditions. Further, any such use must comply with the University policies and other requirements for which such use has been permitted.

2.5. **Confidentiality, Integrity and Availability (CIA) of ICT Resources**

Users must respect and maintain adequate level of confidentiality, integrity and availability of information and ICT resources.

2.5.1. **Confidentially**: Unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept of data privacy must be honored by each user.

2.5.2. **Integrity:** No user should attempt to vandalize, damage or change any data inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the University's ICT resources shall be a clear violation of the University policy.

2.5.3. **Availability:** No user should attempt to affect the availability of ICT resource, whether accidently or deliberately.

2.6. **Extension of ICT (Usage) Policy**

Retaining the consistency in compliance of the Information and Communication Technology (ICT) (Usage) Policy, HNBGU, individual department(s), school(s), individual unit(s), etc. may further define and implement additional "conditions of use" for ICT resources under their control. It will be the responsibility of the department/ school/unit to publicize and enforce such conditions of use. In cases where use of external networks is involved, suitable policies can be practiced in compliance with the broad prerogatives of (Usage) Policy of the University.

2.7. **Access of Information to Legal and Institutional Bodies**

As a part of certain investigation procedures, the University may be required to provide its ICT information, resource and/ or records, in parts or full, to third parties. Also, for proper monitoring and optimal utilization of University's ICT resources, the University may review, analyze and audit its information records, without any prior notice to its Users. Further, the University may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on the University's ICT resources.

3. **ICT Resource Management**

Management and operation of ICT resource will be the responsibility of the university designated officer, such as System Manager, or Dean of Engineering and Technology, or Head of CSE or IT department, or a committee of such officers, who will be named as 'ICT resource administrator'. Under the control of this Officer/committee, concerned head of respective department/School/Division to which that ICT resource belongs will also be responsible to maintain and operate its ICT resources. Compliance of the University's Information and Communication Technology (ICT) (Usage) Policy shall be the sole responsibility of the aforesaid officials for the ICT resources of their concern. For convenience, aforesaid officials may designate another person to manage and operate respective ICT resource (designated as "ICT resource administrator") but responsibility for policy compliance on respective ICT resources shall still remain with the concerned official only. The ICT resource administrator will manage and operate ICT resources as per the

policies of the University and of the concerned sub-division. ICT resource administrator will report to the competent authority of the university (who will act as the Chief Information Security Officer), in any matter, related with maintenance and operation of its ICT resources, or on any related issue(s).

3.1. **System Administration:** The ICT resource administrator/ officers will also carry out the followings:

3.1.1. Educate users regarding various nuances of University's ICT (usage) policy and other prevailing national and international policies and developments.

3.1.2. Help users to implement and comply with the University policies and help users execute and maintain faithfully all licenses on their ICT resource.

3.1.3. Secure and protect ICT resources by taking befitting actions.

3.1.4. Prevent and protect ICT resources from damage or theft.

3.1.5. Coordinate with the competent authority of the university (who will act as the Chief Information Security Officer) to seek recommendations and guidelines for implementation, and to find and correct problems associated with the systems and network under their control.

3.2. **Loss of Use** (Privileges and Suspension of User Access): Consequent upon any inappropriate usage (abuse) of ICT resources or in cases of repeated offences of abuse, it will be the sole prerogative of the ICT resource administrator to temporarily suspend or permanently terminate any user's access to ICT resources, with (preferred) or without (if required urgently) any prior warning to the user. However, after taking such a preventive measure, such cases shall be referred to competent authority and with information to the concerned user.

3.3. **Division of ICT Resource management:** The whole ICT Resources (Human Resources and ICT Equipment) will be divided into two divisions **Software Development Cell** and **Hardware Maintenance Cell** according to their nature. The Software Development Cell will responsible for design and development of all the software applications as per requirements. All the programmers and system analysist will be the part of this cell. The Hardware maintenance cell will be responsible for maintain the hardware and networking infrastructure of ICT. Network administer and technical assistant will be the part of this cell.

4. **Disabling ICT Resource/ User's network connectivity**

4.1. **Network Infrastructure Liability:** The University will hold responsibility of managing and protecting the HNBGU network(s) against electronic forms of attack or abuse. It is the sole prerogative of the University to terminate network connections to computers within its domain due to suspected or actual abuse of the network and/or its components.

4.2. **Termination of Connection to an Offending Computer:** The network connection to an offending computer may be terminated by disabling the port of that particular switch which connects the offending computer to communicate with the Internet and further traffic to and from that computer will be stopped. Local applications on the computer, however, will remain unaffected after such termination.

4.3. **Terminating a Connection with warning:** Depending upon the urgency of taking preventing action(s), concerned Users will be informed regarding their machines which are causing disturbances and an action from the user end will be solicited within a specified time-frame beyond which action can be taken from the ICT resource Administrator's side.

5. Reporting and Investigations of Policy Violations

5.1. **Reporting of Policy Violations:** It is the duty of users to report policy violation(s) before appropriate authority or a concerned official, especially when issues are related with Information and Communication Technology (ICT) (Usage) Policy violation, accounts, system security, or when they have information about unlawful or suspected abuse of ICT resources, through e-mail or in person, during normal office hours.

5.2. **Inspection of ICT Resource and Information Records:** In the interest of better safety of user(s) or the user community, appropriate policy compliance or due to legal proceedings, all or part of ICT resources may be monitored and/ or analyzed or audited with or without any prior notice to any or all the users, by the University or through third-party service providers. Only the Vice-Chancellor of the HNBGU (or his/ her designate) may permit this type of exhaustive inspection and monitoring.

5.3. **Teamwork and Cooperation:** The University solicits wholehearted cooperation and sincere support from its users of ICT resource during any investigation of policy abuse and/ or cyber crime. Instances of non-cooperation from any user shall constitute the grounds for suspension or cancellation of access to ICT resources or other disciplinary actions.

6. **Non-compliance of Policy and Consequent Abuse**

Non-compliance of the Information and Communication Technology (ICT) (Usage) Policy and consequent abuse of ICT resources may attract appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. Violation of this policy may also indicate that a user may also have violated the legal prerogatives as permitted under prevailing cyber laws and acts. If established, such action may also lead to severe civil or criminal proceedings as per the applicable laws and provisions. The ICT resource administrator will refer such violations to the cognizance of the competent authority of the University for seeking further necessary direction(s)/ order(s).

Annexure-1

User Name:
Father's Name:
Mother's Name:
Date of Birth:
Aadhar No.:
Phone No.: Phone No. Linked with Aadhar No.:
School:
Course:
Semester: Year:
Roll No.:
University Enrollment No.:
Present Address:
Permanent Address:

I want to use ICT resources of University in compliance with Information and Communication Technology (ICT) (Usage) Policies of University.

- I will not try to gain or enable unauthorized access to forbidden ICT resource on the University's network.
- I will use only my identity to use ICT resources of University, not of other's.
- I will not access other's copyrighted materials (data, programs or any other digital material, passwords, etc.).
- I will not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material(s) that are a violation of applicable law.
- I will not use unlawful file sharing, any form of illegal or pirated or un-licensed software, on the University's ICT resources.
- I will adhere with the norms as prescribed by social networking websites, applications, mailing lists, chat rooms, blogs, etc.
- I will not use ICT resources for any commercial purpose without permission of university's authority.
- I will use my one smart phone having IMEI No. …….. And Laptop/Desktop Computer having MAC address……..
- I will not make any attempt knowingly or by an accidently that affect the availability of ICT resources.
- I know that for monitoring, optimal Utilization and Investigation University may review, analyze and audit my information/data records, without any notice.
- I know for inappropriate usage (abuse) of ICT resources may attract disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. My access to resources can be suspended or permanently terminated.