



गुरुकुल काँगड़ी (समविश्वविद्यालय), हरिद्वार, उत्तराखण्ड
Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand
(NAAC "A" Grade Accredited Deemed to be University u/s 3 of UGC Act 1956)

IT Policy

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. 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 earthing and have properly laid electrical wiring.

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.

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.

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). University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

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.

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.



गुरुकुल काँगड़ी (समविश्वविद्यालय), हरिद्वार, उत्तराखण्ड
Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand
(NAAC "A" Grade Accredited Deemed to be University u/s 3 of UGC Act 1956)

Network connectivity provided through the University is governed under the University IT Policy. The Network Operations Centre (NOC) 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 NOC.

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. Non-compliance to the 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.

NOC takes no responsibility for the content of machines connected to the Network, regardless of those machines being university or personal property. NOC 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. Network traffic will be monitored for security and for performance reasons at NOC.

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.

Departments, or sections must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the administrators, it is recommended to utilize the university's e-mail services, for formal university communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, 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. For obtaining email account, user may contact Computer Centre for email account and default password by applying in a prescribed proforma.

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



गुरुकुल काँगड़ी (समविश्वविद्यालय), हरिद्वार, उत्तराखण्ड
Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand
(NAAC "A" Grade Accredited Deemed to be University u/s 3 of UGC Act 1956)

1. the facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. 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.
3. 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.
4. 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.
5. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
6. Impersonating email account of others will be taken as a serious offence under the university IT security policy.
7. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

The University has campus network and Wi-Fi facility with NKN 1 Gbps connectivity. Old and outdated computers are upgraded periodically. They are either replaced or enhanced with respect to configuration. Additional computing facilities are added based on the need arising out of requirements of students, research scholars and faculty.