GHARDA INSTITUTE OF TECHNOLOGY

IT Policy

IT Policy refers to a set of rules and guidelines that govern the use, security, and management of an organization's information technology resources.

IT Policy outlines the guidelines and regulations for managing, securing, and using an organization's IT resources. It covers data protection, network security, software usage, and user responsibilities to ensure compliance, prevent misuse, and maintain system integrity.

GHARDA INSTITUTE OF TECHNOLOGY

Purpose of IT Policy

- To maintain, secure, and ensure legal and appropriate use of Information Technology infrastructure established by the College on the campus.
- To establish College-wide strategies and responsibilities for protecting the information assets that are accessed, created, managed, and/or controlled by the College.
- To work as a guide to stakeholders in the usage of the College's computing facilities, including computer hardware, software, email, information resources, intranet, and Internet access facilities.
- To set direction and provide information about acceptable actions and prohibited actions or policy violations.

Scope of IT Policy

- College IT Policy applies to technology administered by the College centrally or by the individual departments, to information services provided by the College administration, by the individual departments, or by individuals of the College community.
- This IT policy also applies to the resources administered by the departments such as the Library, Computer Labs, Laboratories, and Administrative Offices of the College.
- Computers owned by individuals or those owned by research projects of the faculty, when connected to the campus network, are subjected to the Do's and Don'ts detailed in the College IT policy.
- Further, all faculty, students, staff, departments, authorized visitors/visiting faculty, and others who may be granted permission to use the College's information technology infrastructure must comply with the Guidelines.
- IT policies broadly concentrate on the following areas:
  - IT Hardware Installation and Maintenance Guidelines
  - Software Installation and Licensing Guidelines
  - Network (Intranet & Internet) Use Guidelines
  - Email Account Use Guidelines
  - Website Hosting Guidelines
  - College Database Use Guidelines
  - Role of Network/System Administrators

IT Hardware Installation and Maintenance Guidelines

- IT Hardware Installation and Maintenance is performed by System Administrators.
- Faculty and departments can submit IT Hardware requirements based on their academic requirements.
- Procurement of IT Hardware should be initiated based on the availability of stock and the requirements submitted by the departments.
- Stock Register should be updated immediately when IT Hardware is procured.
- IT Hardware Installation and maintenance services are provided only after receiving approval from the concerned Head of the Department and the Principal.

1

- Maintenance of Computer Systems should be done periodically by System Administrators and recorded in the Maintenance Register.
- Movement of IT Hardware within the college or outside the college should be recorded in the Movement Register.
- The major e-waste such as written-off instruments/equipment, Monitors, Printers, Computers, and batteries should be sold regularly.
- The Faculty or the Department is solely responsible for the IT Hardware provided to them, and any damage, loss, or theft needs to be addressed by them.

Software Installation and Licensing Guidelines

- College IT policy allows authorized and open-source software installation on College computers. In case of any violation, the College will hold the Department/Individual personally responsible.
- Open-source software should be used in their systems wherever possible.
- Licensed software needs to be installed in the systems.
- Antivirus software needs to be procured and installed in the systems.
- Backups of data should be taken periodically by the system administrators and stored in an External Hard Disk(NAS) of prominent locations.
- Software used for academic and administrative purposes should be authentic.

Network (Intranet & Internet) Use Guidelines

- Any computer (PC/Server) that will be connected to the College network should have an IP address assigned by the System Administrators.
- An IP address allocated for a particular computer system should not be used on any other computer.
- Changing the IP address of any computer by staff or students is strictly prohibited.
- Configuration of a network will be done by System Administrators only.
- Individual departments/individuals connecting to the College network over the LAN may run server software only after bringing it to the knowledge of the System Administrators.
- Access to remote networks using the College's network connection must comply with all policies and rules.
- Internet and Wi-Fi facilities should be used for academic and administrative purposes only.

Email Account Use Guidelines

- Every faculty member is provided with an email account.
- The email facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the email facility for illegal/commercial purposes is a direct violation of the College's IT policy and may entail withdrawal of the facility.
- Faculty should refrain from intercepting or trying to break into others' email accounts, as it infringes on the privacy of other users.

- Impersonating the email account of others will be taken as a serious offense under the College IT security policy.
- It is ultimately each individual's responsibility to keep their email account free from violations of the College's email usage policy.

Website Hosting Guidelines

- The College Website should be used to provide academic and administrative information for its stakeholders.
- The Website Updation Committee is responsible for content updation and maintenance of the website.
- Maintain up-to-date pages. Proofread pages and test links before putting them on the Web.
- The content hosted on the website should be correct and clear.
- Departments and Associations of Teachers/Employees/Students may have an official Web page on the Website, which must conform to the College Website Creation Guidelines.
- LMS can be linked to the website so that Faculty may post class materials on the Web to facilitate eLearning.
- The Website Updating Committee needs to take proper measures in safeguarding the security of the data hosted on the website.

College Database Use Guidelines

- The databases maintained by the College administration under the College's e-Governance must be protected.
- The College is the data owner of all the College's institutional data generated in the College. Individual or departments generate portions of data that constitute the College's database. They may have custodianship responsibilities for portions of that data.
- The College's data policies do not allow the distribution of data that is identifiable to a person outside the College. Data from the College's Database, including data collected by departments or individual faculty and staff, is for internal College 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 College 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 IQAC Office of the College.
- Requests for information from any courts, attorneys, etc., are handled by the Office of the College, and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the IQAC Office of the College 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.

- All reports for UGC, MHRD, and other government agencies will be prepared/compiled and submitted by the Dean, IQAC coordinator, Controller of Examinations, and Finance officer of the College.
- Tampering with the database by the department or individual user comes under violation of IT policy. Tampering includes, but is not limited to, certain violations of IT policy laid down by the College. Any College member violating these policies may face disciplinary action by the College authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Responsibilities of Network/System Administrators

- Design College Network and perform Backbone operations.
- Follow Global Naming & IP Addressing conventions.
- Review the existing networking facilities and assess the need for possible expansion.
- Configure and maintain Wireless Local Area Networks.
- Configure and maintain IT facilities provided in classrooms, Labs, and Seminar Halls.
- Receive and address complaints from users of the College network.
- Maintain servers in the server room.
- Look into the maintenance of Computer Hardware, Peripherals, and Networking devices.
- Discourage installing any unauthorized software on the computer systems of the users.
- Strictly refrain from obliging unauthorized software installation requests.

E-waste Management

- The Institution has undertaken several E-waste Management initiatives to create an eco-friendly environment on the campus.
- Electronic goods are put to optimum use; minor repairs are set right by the Laboratory assistants and teaching staff, while major repairs are handled by the Technical Assistant and reused.
- Old configuration computers and LCD Projectors are transferred to schools run by our education society.
- Major e-waste such as written-off instruments/equipment, CRTs, and Printers are sold.
- UPS Batteries are recharged/repaired/exchanged by the suppliers.
- All miscellaneous e-waste such as CDs, batteries, and electronic items are collected from every department and office for safe disposal.
- The waste compact discs and other disposable non-hazardous items are used by students for decoration.
- Awareness programs have been undertaken in the institution where students are made aware of E-waste management techniques.