

CT Group of Institutions, General IT Policy

January 2019

Version 3.0

Users of **CT Group of Institutions** are bound by the following policies to use the computing facilities:

Registration to use the Facilities

The use of the facilities is a privilege granted to selected staff, faculty and registered students with the CT Group of Institutions. No member of the institute or other individuals has the automatic right to use these facilities and access may be withdrawn at any time by the designated authority. Access may be granted for other users at the discretion of the designated authority and everybody has to ensure that use of computers, telephones, email and the Internet are provided for work-related purposes, whilst personal use is subject to few restrictions, any personal data stored within the facilities, we provide should not be considered confidential.

Passwords

No one is allowed to share his/her Internet access ID user name and password with others. Access to networked facilities and other systems is given in the form of Username(s) and Password(s). Users are explicitly prohibited from exposing their passwords to third parties. Passwords must never be written down. Passwords should be changed immediately after providing by the IT Team of CT Group. Users must never allow another person to use their account or use the account of another person. Users may be held responsible for the actions of and any consequences of, any other individual using their account. . Users /or System Technical Support team may be required to change passwords or security settings at the request of the Director of **CT Group of Institutions or HOD of CSE Department**, if there is a possible security risk. network administrator/ IT Helpdesk should immediately change all the officials passwords, email id's etc. of the staff and faculty upon leaving the **CT Group of Institutions**, all the passwords should return or laptops and/or portable equipment to the IT Helpdesk.

Viruses and Malicious Code

Users must not interfere with the operation of the Anti-Virus software or change its configuration, unless the designated authority has granted permission. **Users must scan all portable media (DVD ROMs, CD ROMs, Pen Drives and External Hard Disk etc.) for viruses' prior to use.**

Intrusion and Hacking

The regulations surrounding network security are laid down in the CT Group of Institutions Network Security Policy. Users must in no way attempt to gain access to internal or external systems to which they have not been granted access. This includes browsing the network drives without authorization. Users must take all reasonable precautions to prevent other persons from using their account to gain access to internal or external systems, which they have not explicitly been granted access. No one is allowed to open any proxy website inside CT Group of Institutions IT Infrastructure. No one is allowed to install any spy or unethical software to any system, laptop, tablet, phone etc. within the IT infrastructure of CT Group. No one is allowed to open any illegal website inside CT Group of Institutions IT Infrastructure. Entire internet or IT related activities are under observation by the IT team of CT Group.

Backup of Data

It is the responsibility of the user to ensure that they should backup all of their own data, whether it be held on local drives (e.g. computer hard drives), or portable media (e.g. pen drives). IT Group does not take responsibility for loss of data due to inadequate backup by users. The **CT Group of Institutions** accepts no responsibility for the loss of data due to malfunctions, neglect, actions or inactions of members of staff, or security breaches. No claim shall be made against the IT team of CT Group for this kind of action.

Laptops and Portable equipment

Laptops and portable devices owned by the **CT Group of Institutions** are subject to the same policies and regulations as desktop machines. Members of staff are responsible for data held on items of portable equipment. Any equipment returned to the helpdesk shall have any data and/or software removed from it. The equipment shall be reused, recycled or disposed of depending upon its age and usability. **Users need to handle the equipments with utmost care and prevent any kind of damage to issued equipment.**

Use of personal equipment

Users do not by default have the right to connect personal equipment to the IT infrastructure of CT Group network. Permission may be granted to connect personal equipment at the discretion of the Director/ Principal/HOD(CSE)/ IT Manager , provided it meets required standards.

Monitoring of IT resources

Software installation and usage is monitored as part of the **CT Group of Institutions** ongoing software audit. All access to computers and network resources is logged and routinely monitored by the IT team of **CT Group of Institutions** staff as part of the day-to-day operation of the network. No expectation of privacy should be taken with regard to emails or Internet use. In accordance with Indian Law, the designated authority may, on behalf of the **CT Group of Institutions**, authorize the monitoring of communications and or access logs.

Reporting misuse or accidental breaches of policy

If, a user accidentally go to, or be redirected to, a website prohibited in the Staff Internet Policy or Student Internet Policy they should inform the Director /Principal/ HOD(CSE)/IT manager of **CT Group of Institutions** of the incident as soon as possible. All individual have reasonable grounds to suspect that a user has broken **CT Group of Institutions** policy on the use of IT, they should immediately contact the Director /Principal/ HOD (CSE)/IT manager of **CT Group of Institutions**. Upon receiving such a report the Director/ Principal on behalf of the institute, authorize the investigation and or monitoring of logs. The result of such an investigation may result in disciplinary proceeding. The designed authority reserves the right to terminate or suspend computing accounts at any time.

If any of the faculty need help regarding the computing facilities, he/she may contact directly to the IT Help Desk or email at systemadmin@ctgroup.in or viceprincipal.ctiemt@ctgroup.in

CTIEMT IT Help Desk: Ext. No - 230

As per our IT POLICY this is to inform you that CT Group of Institutions to circulate the given below message to entire students, staff and faculty members. All the individuals should have the awareness that their entire internet access or IT related activities are observed and continuously monitored by CT Group of Institutions (IT Team). If, we found anyone doing any of these unauthorized activities inside CT Group of Institutions IT Infrastructure then he or she should ready to face any consequence from CT Group of Institutions.