№ 014915

0181-2343400, 2207650
Tel/Fax : 0181-2205851,2205852
e mail : daviet@davietjal.org

www.davietjal.org

D.A.V. INSTITUTE OF ENGINEERING & TECHNOLOGY
(DAVIET)

KABIR NAGAR, JALANDHAR. - 144008
(ISO 9001:2008 Certified)

Approved by : All India Council for Technical Education, New Delhi & Govt. of Punjab
Affiliated to : Punjab Technical University, Jalandhar
Managed by : DAV College Managing Committee, New Delhi

Ref. No. DAVIET/ Estt/2016-17/906

Dated 23-3-2017

Office-Circular

The Governing Body of DAV Institute of Engineering & Technology, Jalandhar, in its 15th meeting, held on 07.12.2016, vide item no. 15.21 has approved the **General IT Policy (Version 1.0) of DAVIET.** All users of DAV Institute of Engineering & Technology are bound to follow this IT Policy to use the computing facilities.

This policy applies to all users of computing resources owned or managed by DAV Institute of Engineering & Technology, Jalandhar. Guidelines and processes for DAVIET access to use electronic information stored in or transmitted through any DAVIET system have been set-out in this policy. This policy applies to all users of DAVIET. Individuals covered by the policy include faculty and visiting faculty, staff, students, alumni, contractors, volunteers, physicians, guests or agents of the administration, and external individuals and organizations accessing network services via the DAVIET computing facilities. This policy applies to Institute's/ personally owned computers and devices connected by wire or wireless to the DAVIET network and to off-site computers that connect remotely to the DAVIET's network services. Laptops and portable devices owned by DAVIET, Jalandhar are subject to the same policy and regulations as desktop machines. Members of staff are responsible for data held on items of portable equipment.

Detailed DAVIET General IT Policy (Version 1.0) is enclosed herewith. **HOD (IT)/ Network Administrator is requested to circulate the same and take signatures of all the users on prescribed performa before providing the access to the users and submit copies of the signed performae in the O/o. undersigned.** It is the responsibility of IT team of DAVIET to ensure that all the individuals should have the awareness that their entire internet access or IT related activities are observed and continuously monitored by DAVIET (IT Team). If anyone is found violating the DAVIET IT Policy, disciplinary action shall be taken against him/her.

(Dr. Manoj Kumar)
Principal

Copy for information & compliance to:-

1. All HoD(s)/Deans/HcD(s)
2. Head (IT)
3. Network Administrator
4. All Computer Lab Technicians/Assistants

DAVIET

GENERAL IT POLICY VERSION 1.0

DAVIET has framed General IT Policy. All Users of DAV institute of Engineering and Technology (DAVIET) are bound to follow this IT policy to use the computing facilities:

This policy applies to all users of computing resources owned or managed by **DAV Institute of Engineering & Technology, Jalandhar,** This policy sets out guidelines and processes for DAVIET access to use electronic information stored in or transmitted through any DAVIET system. This policy applies to all users of DAVIET. Individuals covered by the policy include faculty and visiting faculty, staff, students, alumni, contractors, volunteers, physicians, guests or agents of the administration, and external individuals and organizations accessing network services via the DAVIET computing facilities.

These policies apply to personally owned computers and devices connected by wire or wireless to the DAVIET network and to off-site computers that connect remotely to the DAVIET's network services. Laptops and portable devices owned by the **DAV institute of Engineering & Technology, Jalandhar** are subject to the same policies and regulations as desktop machines. Members of staff are responsible for data held on items of portable equipment.

Registration to use the Facilities

The use of the facilities is a privilege granted to staff, faculty and registered students with the DAVIET. 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. All the users must ensure that use of computers, telephones, e-mail(s) 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 personal or confidential. Access may be granted for other users at the discretion of the Principal /designated authority and he or she may be treated as a **guest user** but record of the guest user should not be considered confidential.

Passwords

No one is allowed to share its **Cyberoam** (Internet Access id(s)) user name and password(s) 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 divulging their passwords to third parties. Passwords must never be written down. Passwords should be changed immediately after securing it from IT Team of DAVIET. 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.

Intrusion / Hacking/ Viruses and Malicious Code

The regulations surrounding network security are laid down in the DAV institute of Engineering &Technology, Jalandhar, **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 install any **spy or unethical software** to any system, laptop, tablet, phone etc. within the IT infrastructure of DAVIET. No one is allowed to open any illegal website inside DAV institute of Engineering & Technology, Jalandhar IT Infrastructure. Entire internet or IT related activities are under observation of the IT team of DAVIET. 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 (floppy discs, CD ROMs, pen drive etc.) for viruses' prior to use or connection with the DAVIET Network.

IT equipment Policy

For any system / laptop/ mobile / hard-disk /USB drive **issued** by the IT department, concerned official shall be responsible for any theft /loss /damage. All the concerned officials should deposit/make-available, the equipment under their charge for the annual physical verification to the IT department or the committee constituted for the purpose. In case one leaves the job of DAVIET, Jalandhar; all the equipment under their charge and passwords should be returned to the IT Team /Concerned HOD. Any equipment returned back to the DAVIET shall be reused, recycled or disposed off depending upon its age and usability**.**

Monitoring of IT resources

Software installation and usage is monitored as part of the 'Software Audit' conducted by DAV institute of Engineering & Technology, Jalandhar. All access to computers and network resources is logged and routinely monitored by the IT team of DAV institute of Engineering & Technology, Jalandhar as part of the day-to-day operation of the network. In accordance with Indian Law, the designated authority may, on behalf of the DAVIET, authorize the monitoring of communications and or access logs of all users of DAVIET. No expectation of privacy should be taken with regard to email(s) or Internet use within the DAVIET network.

Use of personal equipment does not by default have the right to connect personal equipment to the IT infrastructure of DAVIET network. Permission may be granted to connect personal equipment at the discretion of the Principal or a designated authority, provided it meets required standards.

System Technical Support team may be required to change passwords or security settings at the order of the Principal or any other competent authority.

Reporting/ misuse or accidental breaches of policy

If any user accidentally go to, or is redirected to, a website prohibited by the IT team of DAVIET, it should be immediately brought into the notice of the Principal/ HOD(CSE or IT)/Network Administrator of DAV institute of Engineering &Technology, Jalandhar. All individual have reasonable grounds to suspect that a user has broken DAV Institute of Engineering and Technology, Jalandhar policy on the use of IT, they should immediately contact the Principal/ HOD(CSE or IT)/ Network Administrator. Upon receiving such a report, Principal on behalf of the institute will authorize the investigation and or monitoring of logs. The result of such an investigation may result in disciplinary action. The designated authority reserves the right to terminate or suspend computing accounts at any time. If any of the employee or student needs help regarding the computing facilities, he/she may contact directly to the IT Help Desk at Ext. No: 451 or email to ithelpdesk@davietjal.org.

Backup of Data

It is the responsibility of the user to ensure that they should keep backup of their data. IT team of DAVIET does not take responsibility for loss of data due to inadequate backup by users. The

DAV Institute of Engineering &Technology, Jalandhar 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 DAVIET this kind of action.

Use of Email Accounts:/ Email Forwarding/ E. Misuse

All the internal and external communication should be done through the registered id(s) which will be treated as Official Email Address. E-mail services are primarily intended to allow faculty and staff to conduct DAVIET business. Personal use of e-mail is allowed, provided that personal use does not materially interfere with performance of DAVIET work. At any time log of e-mails can be evaluate. Users have no control over the forwarding or alteration of email(s) once they are sent. Accordingly, users must not use email to communicate / transfer any material which is related to DAVIET. Although the DAVIET does not monitor email content routinely, users must not assume that email content will remain private and confidential. A user's expectation of privacy in Emails is defined and limited by the IT Policy. Access to email by anyone other than the user may be permitted as described in that Policy. In addition, email can be altered or forwarded by a recipient without the sender's knowledge. Fake e-mail id(s) may also be discoverable in litigation. IP(s) will be traceable in case of any unauthorized activities inside the network, Network Administrator should have the record of that user and the provide the proof for the same and case may be registered under the Cyber-Crime and in addition, a violation may result in:

- Suspension, blocking, or restriction of access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of DAVIET resources .
-
- Disciplinary action up to and including separation from the DAVIET.

Code of Conduct and Responsibility of the IT Team/ Network Administrator / Lab Instructor(s)

As per our IT Policy this is the responsibility of Head, Department of IT/ Network Administrator to take the signatures of the users on prescribed Performa before providing the Access to the users. Also it is the responsibility of the IT team of DAVIET to ensure that all the individuals should have the awareness that their entire internet access or IT related activities are observed and continuously monitored by DAVIET (IT Team). If anyone is found violating the DAVIET IT policy, disciplinary action shall be taken against him/her. Network administrator is responsible for taking complete backup of the required data periodically and to make the same available to Principal or any other competent authority as and when required. All lab technicians should keep the proper record of the users on the lab registers along with the correct time in/out. No faculty/ staff / guest user can sit in the lab without making the entry on the lab registers. If there is a possible security risk, Network Administrator/ IT Helpdesk should immediately take necessary action viz. changing the official passwords etc. Network Administrator should record all the necessary information of the individual before issuing ID or password or allocating IP.

(Sd/-)
Principal
DAVIET, Jalandhar