Computer and Network Use Policies

ACCEPTABLE USE POLICY

1.0 Overview

The P.A.Inamdar College of Visual Effects,Design & Art (Hereafter “Veda College” Office of Information System's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Veda College's established culture of openness, trust, and integrity. Information Systems is committed to protecting Veda College's students, faculty, users, partners, and the College from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Veda College. These systems are to be used for approved purposes in serving the interests of the College, and of our users in the course of normal operations. Please review user policies for further details.

Effective security is a team effort involving the participation and support of every Veda College user and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Veda College. These rules are in place to protect the user and Veda College. Inappropriate use exposes Veda College to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to students, faculty, users, contractors, consultants, temporaries, and other workers at Veda College, including all personnel affiliated with authorized third parties. This policy applies to all equipment that is owned or leased by Veda College as well as any third party equipment using the Veda College network infrastructure for any reason.

4.0 Policy 4.1 General Use and Ownership

1. Because of the need to protect Veda College's Network, management cannot guarantee the confidentiality of information stored on any network device belonging to Veda College or transmitted in any way across the Veda College network infrastructure.
2. Users are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, users should be guided by departmental policies on personal use, and if there is any uncertainty, users should consult their Head of Dept. or Dean.
3. Any user using a privately owned computer, Laptop or College-owned computer will have to register his/her device with the College's registration system and will

then have to authenticate using his/her user account in order to use any available network resource.

4. The College has the right to allow or deny access to some or all of the network resources to any user. The final determination will be made by Veda College management.
5. For security and network maintenance purposes, authorized individuals within Veda College may monitor equipment, systems, and network traffic at any time.
6. Veda College reserves the right to audit networks and all systems connected to the Veda College network infrastructure in any way on a periodic basis to ensure compliance with this policy.

4.2 Eligible Network Users

1. Students must be registered at the College in order to create and maintain a network account whether or not a Veda College email address is being created.
2. Employees must be cleared and verified by Human Resources as active employees in order to create and maintain a network account.
3. All other network users must go through their department's approval process before Information Systems will create and maintain their network account.

4.3 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, and user level passwords should be changed every six months.

2. All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
3. Postings by users from a Veda College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Veda College, unless posting is in the course of business duties.
4. All hosts used by the user that are connected to the Veda College Internet/Intranet/Extranet, whether owned by the user or Veda College, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
5. Users must exercise extreme caution when opening email attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a student or employee of Veda College authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Veda College-owned resources or infrastructure.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Veda College or the individual user.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Veda College or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, malwares etc.).

Revealing your account password to others or allowing use of your account by others.

This includes family, colleagues, and other household members when work is being done in on- or off-campus locations.

5. Using a Veda College computers asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any Veda College account.
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless performed by Information Systems to assess security conditions.
10. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).

13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of, Veda College users to parties outside Veda College.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Veda College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Veda College or connected via Veda College's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

8. For more details Students and employees must carefully read our separate Email Policy and abide by the same.

Monitoring Information to the Public or college owned devices

The college administration can monitor the information that is being accessed on college owned computers and Internet devices through monitoring, screen capture or keyboard recording applications for security purposes. This monitoring will not be announced and can be executed at any time with any device you are which is owned or rented by college.

Applicable from 1st Sept 2020