WIRELESS COMMUNICATION/ WIFI POLICY

1.0 Purpose

This policy prohibits access to Veda College networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Systems are approved for connectivity to Veda College networks.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Veda College's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Veda College networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the College network must be registered and duly approved by The Network and System Administrator Office (NSAO) and Principal of the Institution. These Access Points / Base Stations are subject to periodic security tests and audits and if it is determined that wireless devices are interfering with the Veda College wireless network and/or its users, NSAO will require that the device be removed. All wireless Network Interface Cards (i.e., PC cards) used in laptops, desktop computers and other network devices must be registered with NSAO.

3.2 Approved Technology

All wireless LAN access must use NSAO-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication

All computers on Veda College's wireless network must be configured with WPA encryption with PEAP authentication or be configured with the Odyssey Client in order to function on the network. All computers with wireless LAN devices must utilize the Veda College Virtual Private Network (VPN) when conducting official College business on an external network. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or similar to that standandards.

3.4 Use of Wi-Fi

Except the explicitly permitted cases with a written approval of the Principal, the teaching, non-teaching staff, students, parents or Guest of college are not permitted to use social media applications over the Wi-Fi.

4.0 Sanctions for Policy Violations

Violations of these policies will be dealt with in the same manner as violations of other College policies and may result in disciplinary review by the College as well as a private cause of action. By such a review, the full range of disciplinary sanctions is available, including the loss of computer use privileges and dismissal from the College.