

Security Policy for the Kentwood Preparatory Virtual Private Network (VPN)

1. Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to the Kentwood Preparatory campus network.

2. Scope

This policy applies to all Kentwood Preparatory students, employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN's to access the Kentwood Preparatory network. The VPN user will also be subject to the conditions and performance constraints of their chosen Internet Service Provider.

3. Policy

Approved Kentwood Preparatory students, employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy.

Additionally:

3.1. It is the responsibility of staff and students with VPN privileges to ensure that unauthorized users are not allowed access to Kentwood Preparatory internal networks.

3.2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong password.

3.3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

3.4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

3.5. VPN gateways will be set up and managed by Kentwood Preparatory network personnel.

3.6. All computers connected to Kentwood Preparatory internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (IE AVG antivirus software) this includes personal computers.

3.7. VPN users will be automatically disconnected from Kentwood Preparatory 's network after sixty minutes² of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

3.8. Wherever practicable, maintenance of the VPN will take place from time to time, thus disabling the user's access to the Kentwood Preparatory network.

3.9. The VPN concentrator is limited to an absolute connection time of 24 hours.

3.10. Users of computers that are not Kentwood Preparatory - owned equipment must configure the equipment to comply Kentwood Preparatory's VPN and network policies.

3.11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Kentwood Preparatory's network, and as such are subject to the same rules and regulations that apply to Kentwood Preparatory-owned equipment, i.e., their machines must be configured to comply with Kentwood Preparatory's Security Policy.

4. Enforcement

Any member of staff or student found to have violated this policy may be subject to disciplinary action.