

## **Resident and Non-Resident Student Network Connectivity Policy**

Applies To:	All students	Policy Number:	ITS-0003
Issued By:	Director of ITS	Policy Version Number:	1.1
Date Issued:	July 5, 2005	Last Review Date:	March 1, 2018
		Last Revised Date:	March 1, 2018

### **Preamble**

It is strongly advised for the protection of your data that your system is equipped with up-to-date virus protection (configured for daily updates) and up-to-date operating system security patches (configured for daily updates). Unprotected systems are highly susceptible to infection and often become infected without any visible signs.

For all resident students, a hard-wired data connection port is available in each room for network connectivity

For students with WIFI capability, a wireless environment exists around the University.

### **Policy**

Any system unfairly using available bandwidth whether deliberately or via compromised system will be immediately disconnected from the network without notice.

Any system using available bandwidth for illegal or improper activities detected will be immediately disconnected from the network without notice.

For faculty, staff and administration, under no circumstances is non-University equipment connected to the network.

### **Regulations**

The University reserves the right to refuse connectivity to users who violate this policy. In most instances the disconnection will remain in place until the infraction has been cleared.

Repeated offenders may be subject to permanent disconnection.