# CONCORD UNIVERSITY
# BOARD OF GOVERNORS

**Policy No. 45**
**Policy on Wireless Network**
**Effective Date: 06/08/2010**

## SECTION 1. General

1.1 Scope:
This policy is required to protect Concord University's network infrastructure from uncontrolled or unauthorized access that could result in intellectual property loss or data destruction and to provide a consistent interface and procedure for use by the Concord community.

## SECTION 2. Purpose:

2.1 Wireless Local Area Networks (WLAN) or WiFi networks are by nature an open transport technology that can be inherently insecure and therefore any extension to the University's networks using this infrastructure must be authorized by Computer Services prior to procurement and implementation.

2.2 Security and access control will be implemented and any visitor to Concord University requiring wireless access may be required to register with Computer Services prior to date needed allowing 24 hours for the request to be processed. Computer Services will work to maintain internet access as open as possible consistent with security requirements.

2.3 Radio propagation and channel management will be controlled by Computer Services to prevent interference and unintentional spill.

2.4 All wireless access nodes added must be approved and configured by Computer Services to ensure appropriate security is enabled and correct operation with existing equipment.

2.5 No wireless device can be used to provide private network services for downstream unregistered user equipment or services.

2.6 Commercial propagation of WiFi services onto the University's sites needs to be formally registered and pre-approved by Computer Services.

2.7 Computer Services will monitor the network for rogue wireless implementations and has the authority to disable and disconnect immediately upon detection.

2.8 Any breach of this policy may result in network privileges being revoked.

2.9 Computer Services will work with departments to accommodate special needs, where technically feasible and cost justifiable. Computer Services will collaborate with academic departments where devices used for specific educational or research applications may require specific solutions.

## Definitions

*Access Nodes:* *This is the device that is connected to the wired network and provides wireless access for devices to resources on the network.*

*Channel:* *A channel is a communications path based on different frequencies that access points and devices can select to communication.*

*Computer Services:* *Concord University's information technology support organization.*

*Protocol:* *This is the communications language used between peers.*

*Radio propagation:* *This is the transmission and reception area covered by the access point where access to service can be achieved.*

*WiFi:* *Acronym for Wireless Fidelity.*

*Wireless devices:* *This is an assortment of electronic devices and could include but is not limited to a computer, tablet, personal digital assistant (PDA) or mobile telephone.*

*WLAN:* *Local area networks that use wireless communication defined by the IEEE 802.11 standard.*

## Audience

All people using Concord University's network infrastructure, including staff, faculty, students, visitors and affiliates.

## Legal compliance

Wireless networking has the potential to make it very easy to gain unauthorized access to the University network based resources. However, the Privacy Act 1993 places an onus on organizations to protect information from inappropriate access by unauthorized parties.

There is a significant amount of information held on the University's network and it is therefore important to ensure that only appropriate people have access to this resource.

## Notes

Adapted with permission from Massey University Policy Guide and Marshall University Wireless Communications and Networking Procedure.