



Policy Title: Information Technology Services – Wireless Network Policy

Policy Number:

Established: January 13, 2006

Approved by: VP Admin & Finance, Provost & VP Academic

Last Approval Date: January 4, 2009

Revision Date: July 2019

Position Responsible for Maintaining and Administering the Policy: Executive Director,
Information Technology Services

Contact: Ryan Kenney, Executive Director, IT Services, (519) 253-3000 ext. 2740

Table of Contents

<u>Item</u>	<u>Page</u>
Policy Statement	2
Purpose	2
Scope	2
Exceptions to the Policy	2
Cross References	2
Definitions	2
Procedures	3
Review Process for Policy	3
Process for Communicating Policy	4
Appendix	4

Policy Statement

This Policy guides the deployment of wireless network technology at the University of Windsor.

Purpose

The objectives are to provide secure and functional wireless network services and to arbitrate possible interference of other wireless devices with the campus wireless network (the UWin Wireless Network).

Scope

Individuals and/or departments must not independently deploy wireless access points in any building serviced by the UWin Wireless System.

This policy governs the deployment and use of electronic devices that operate in any license-exempt radio frequency band used for high speed wireless network connectivity, specifically in the 2.4 and 5 GHz range as set by Industry Canada and applies to both the indoor and outdoor use.

Exceptions to Policy

None

Cross-References

Information about obtaining a personal or guest UWin ID and password is available at www.uwindsor.ca/uwinid. Policies pertaining to examination procedures may be found at: www.uwindsor.ca/senate under Senate Policies E3 and E4.

Definitions

Wi-Fi®, or Wireless Fidelity, or 802.11 a/b/g/n/and future protocols

- a protocol that allows you to connect to the Internet from virtually anywhere where the service is available.

UWin Wireless Network

- a local area network technology that uses a range of radio frequencies to wirelessly connect computing devices to an Access Point on the campus network.

Access Point

- a wireless communications hardware device that creates a central point of wireless connectivity. The total bandwidth is shared among all users for which the device is maintaining an active network connection.

Wireless Network Interface Card (NIC)

- a user-supplied wireless communications hardware network adapter contained within each user's computing device that will allow access to the Wi-Fi® networks.

Interference

- refers to the degradation of a wireless radio signal caused by electromagnetic radiation from another source. Interference can slow or eliminate a wireless transmission depending on the strength of the interfering signal

Procedures

Preamble

Wi-Fi®, or Wireless Fidelity, allows you to connect to the Internet from virtually anywhere. Wi-Fi-enabled computers and handsets use radio technologies based on the IEEE 802.11 standard to send and receive data anywhere within the range of a base station.

Implementing a Wireless Networking solution allows for a comprehensive wireless coverage area, simple access, enhanced security, and the ability to roam between access points. Using the 802.11a/b/g/n and future wireless LAN standards, users will be able to connect their laptop, desktop and mobile devices to the Internet through the campus network. At this time, although 802.11b and g are supported, 802.11a is the preferred technology in areas where the concentration of users could be high.

Statements

1. All Acceptable Use provisions and protocols as prescribed will apply to the wireless network services.
2. IT Services will be the sole provider of design, specification, installation, operation, maintenance and management services for all wireless access points connected to the University network in consultation with other islands of technology within the University community.
3. IT Services will work with the affected clients to mitigate interference and accommodate devices without disrupting the UWin Wireless Network. In the event that interference cannot be resolved, the UWin Wireless Network will have priority. Other wireless devices that use the frequency bands used by Wi-Fi® may disrupt the operation of the UWin Wireless Network. These include cordless phones, microwave ovens, cameras, keyboards, mice, audio speakers, and other wireless LAN devices. If interference occurs between other devices and the UWin Wireless Network, the UWin Wireless Network will have priority. In cases of significant problems, users will be required to cease using those devices.
4. All users of the UWin Wireless Network will be required to have an activated UWin ID and password which will be used to authenticate to the UWin Wireless Network.
5. Individuals and/or departments must not independently deploy wireless access points.

Review Process for Policy

This Policy will be reviewed every 5 years. Under the following circumstances, this Policy may be reviewed before the 5 year term: changes in legislation that affect the Policy; a specific incident triggers a review of the Policy; there is a request made by senior management or the Board of Governors to review the Policy.

Process for Communicating Policy

The Policy will be posted on the University of Windsor's IT Services website, within two weeks of the approval of the Policy. Separate notifications may also be sent via e-mail or other means to Departments directly affected by the Policy, or in some cases, the broader campus community if deemed applicable.

Contact Information

Inquiries regarding the policy should be directed to Executive Director, IT Services or appropriate individual in the Department where the policy was developed, as per the contact information at the introduction of the Policy.

Appendix

None