

# Wireless LAN Communications Policy

Publication Date: September 11, 2006

Effective Date: September 11, 2006

Office of Accountability: VP Administration

Administrative Responsibility: Director, IT Services

Approver: VP Administration

## 1. Purpose

This policy provides guidelines and direction for wireless communications on the OCAD network. The goal is to ensure reliable and secure wireless access for the entire OCAD community without impeding the regular day-to-day security and function of other OCAD communication technologies.

## 2. Scope

This policy applies to all users, devices and applications using wireless communications on the OCAD campus, using 802.11 standards and any encryption for wireless data.

## 3. Policy

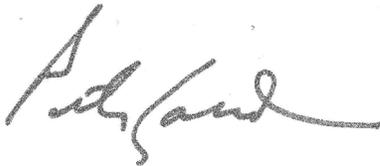
OCAD's goal is to provide the highest possible quality of wireless networking service to users. The following guidelines and general information have been established to assist in this goal:

- i. OCAD IT Services is responsible for the deployment, administration, support and security of all wireless networking services on campus.
- ii. The use of the OCAD wireless network is subject to the university's Acceptable Use Policy, which is available for review at [www.ocad.ca/current\\_students/acc.htm](http://www.ocad.ca/current_students/acc.htm), as well as the OCAD Code of Student Conduct, viewable at [http://www.ocad.ca/current\\_students/registrarial\\_services/policies\\_regulations.htm](http://www.ocad.ca/current_students/registrarial_services/policies_regulations.htm).
- iii. All access to the wireless network must be authenticated with a valid OCAD login and password. Unauthorised network access is prohibited.
- iv. Network users are required to connect via an 802.11g network card with a computer running Mac OS X (version 10.3 or greater; 10.4 preferred) or Windows XP. Windows XP users must run up-to-date anti-virus software, and, to the extent possible, ensure that their operating system is fully patched.
- v. Deployment of unauthorised wireless access points is prohibited. OCAD IT Services will scan for rogue access points and block network connectivity to those detected. Set up of any such unauthorised wireless access points will be considered a violation of the OCAD Acceptable Use Policy and followed-up accordingly.

- vi. Any equipment that operates in the wireless frequency spectrum must be configured to avoid interference with the OCAD wireless or other network signals. If the equipment creates interference affecting the performance or security of OCAD network services, OCAD IT Services may prohibit the use of the device.
- vii. Networking services, including wireless access, for OCAD research activities shall be governed by specific Service Level Agreements (SLA) between the research body and OCAD IT Services (to be negotiated on a case-by-case basis). Any such SLA will supersede this policy, as applicable.

#### **4. Implementation**

The Director, IT Services is responsible for the implementation and enforcement of the OCAD Wireless LAN Communications Policy and any violations will be governed by the “Complaint and Violation Resolution Process” outlined in the OCAD Acceptable Use Policy.

A handwritten signature in black ink, appearing to read "Peter Caldwell". The signature is fluid and cursive, with a long horizontal stroke at the end.

Peter Caldwell  
Vice President, Administration

September 11, 2006