



Canada's Capital University

<b>Policy Name:</b>	Radio Frequency Interference
<b>Originating/Responsible Department:</b>	Information Technology Services (ITS)
<b>Approval Authority:</b>	Chief Information Officer (CIO)
<b>Date of Original Policy:</b>	May 2012
<b>Last Updated:</b>	May 2012
<b>Mandatory Revision Date:</b>	May 2017
<b>Contact:</b>	Director, Operations and Infrastructure, ITS

**Policy:**

ITS provides campus wireless network services to the University community and will attempt to ensure that RF (Radio Frequency) interference does not negatively impact these services. If RF transmissions from other sources interfere with the campus wireless network, the campus wireless network will have priority.

**Purpose:**

This Policy will support the delivery of reliable and secure campus wireless network services to the University community. It outlines how ITS resolves interference problems from other radio frequency sources on campus in order to prevent performance and security problems for users connecting to the campus wireless network. The Campus Wireless Network is any public or private wireless network managed and configured by ITS.

**Scope:**

This policy applies to the use or deployment of electronic devices that operate in any unlicensed RF band used for wireless network connectivity. These include the 2.400-2.483, 5.15-5.35, 5.470-5.725, and the 5.725-5.825 GHz bands. This Policy applies to all areas on campus where ITS provides wireless coverage.

**Procedures:**

1. If ITS detects interference with the campus wireless network, or with teaching or research activities, ITS may act to track, identify and evaluate devices that might be causing the interference, and in doing so may request that any device causing interference:
  - Not be used and be disconnected and/or powered off until the interference is eliminated
  - Be temporarily deposited with ITS for testing and evaluation
2. Following the execution of the procedures outlined in number one, if ITS determines that a device continues to interfere with the campus wireless network, or with teaching or research activities, and is causing any of the following problems:
  - Security or confidentiality concerns
  - Concerns about theft of hardware or misuse of services

- Reliability issues (which may cause data loss, or effect bandwidth, speed, coverage, up- time, and security of the network)
- Significant maintenance or operating costs

ITS may then act to address the problem by:

- Disabling services or access points
- Disconnecting the device or cables
- Requiring removal of the device and/or temporary deposit of the device with ITS
- Agreeing to undertake, at the request and cost of the owner or operator of the device, to alter the campus wireless network or the device to address any of the problems outlined above

ITS must return any device on deposit with it upon demand of the device owner. Devices on deposit with ITS for longer than 2 years will be deemed abandoned.

**Compliance:**

Non-compliance with this Policy may result in disciplinary action.

**Contacts:**

Director, Operations and Infrastructure, ITS

**Links to related Policies:**

<http://carleton.ca/secretariat/policies/>

- Acceptable Use Policy for Information Technology (IT)
- Information Technology (IT) Security