383 Birch Street North
Timmins, ON  P4N 6E8
Phone: (705) 268-7443
Fax: (705) 267-3590
Toll Free : (877) 422-9322
www.ncdsb.on.ca

NCDSB

**NORTHEASTERN CATHOLIC DISTRICT SCHOOL BOARD**

# *Personal Network Devices*

## *Administrative Procedure #:  API002*

## References

- Board Policy

  I-4: Personal Network Devices

## Procedure

### 1. ADMINISTRATIVE PROCEDURE

1.1. Principals will ensure that students or employees using a personal network device (the Device) have completed the Responsible Use of Computer Technology and the Internet Agreement Form and will maintain a copy of the form in the school's files. An electronic acknowledgement of the Policy may also serve as the official record in lieu of a paper copy; this will be at the discretion of the principal.

1.2. Users of the Device agree that, while the Device is on Board property, they are bound by the Board's Responsible Use of Computer Technology and the Internet Policies, specifically Policy XXX for employees and for students. Home use for students may also be subject to the "Nexus" provision of Policy XXX, Safe Schools - Code of Conduct.

1.3. The Policy will apply to all Devices that are able to connect to the Board's network. Multi-radio devices such as those found in some cell phones are also covered under the Policy if they choose to use the wireless radio feature to connect to the Board's wireless network and if they use the wireless radio feature linked to an available cellular service provider.

1.4. The Board will not service the Device.

1.5. The Board will not be responsible for the loss, damage, or theft of the Device.

1.6. Access to the NCDSB_Public Network using the Device is at the discretion of the 'principal' at the specific school location.

1.7. The Manager of Information Technology will oversee the Device access at the board office.

1.8. The Information Technology Department and/or the Senior Administration and/or the Board may determine the:

1.8.1. type of access provided (wireless, wired, or no access)
1.8.2. suitability of any device to be connected
1.8.3. resources available when connected (internet only, local web, and/or server access).

1.9. In determining network access, the Information Technology Department and/or the Senior Administration and/or the Board reserves the right to:

1.9.1. monitor all network activity to and from the Device
1.9.2. monitor volume of network traffic from a Device and limit the traffic if deemed necessary log network activity, including internet access to and from the Device perform system scans to evaluate the security level of the Device including, but not limited to, the update status of Antivirus, Spyware, and system components
1.9.3. perform system scans to determine compliance with the Board's Responsible Use of Technology and the Internet Policies and applicable laws
1.9.4. perform a physical inspection of the system

1.10. No student or employee will connect a Device to the Board's network which allows network access over and above what is provisioned by the Board. These Devices include, but are not limited to, modems, routers, wireless access points, cellular modems.

1.11. Use of the Device in the school is a privilege granted at the discretion of the school principal. The student use of the Device at particular times in individual lessons is at the discretion of the teacher.

1.12. No internal components belonging to the Board shall be placed in any Device, whether as enhancements, upgrades, or replacements.

1.13. Users will not install software licensed by the Board or the Ministry of Education on the Device unless they are legally entitled to do so by having purchased the software. The only exception to this procedure is software

1.14. licensed for home use by teachers or students. A list of this software is available at the home page for the Ontario Software Acquisition Program.

1.15. Users will ensure that the Device is updated with software and/or firmware updates as recommended by the manufacturer. Users will also ensure that, where applicable, the Device has antivirus software installed and that the definitions for the software are up to date. Failure to do so may result in network access being revoked.

1.16. Users will not run or host servers on their Device. This includes, but is not limited to, web servers, ftp servers, e-mail servers, file sharing, and peer to peer software.

1.17. If a Device is found to be interfering with the operation of the Board's Information Technology systems, users may be required to provide their Device to the Board for an inspection of the Device.

1.18. Users will not use the Device to store "personal information" as defined in the Municipal Freedom of Information and Protection of Privacy Act.

## 2.0 TERMS AND DEFINITIONS

PERSONAL NETWORK DEVICE
A personal network device is a device, owned by the user, which has the capability to connect to a computer network, either through a network wire or using a radio designed to connect to a wireless computer network.
Examples include: laptops, netbooks, some portable music players, some portable game devices, and some cellular telephones.

MULTI-RADIO DEVICE
A multi-radio device is a network device which employs more than one radio to connect to multiple networks. Some cellular telephones will allow users to choose whether they connect to a cellular network or to a
computer network in order to access the internet.

NEXUS
The umbrella for "school behaviour" includes matters which fall under the category of "nexus". Nexus means "relevant". The student's behavior off school property and/or outside the school day may have a relevant and
related impact on the safety and well-being of the school community.

WEB SERVER
A web server is a computer program that serves the requested files which form web pages to the client's browser.

FTP (FILE TRANSFER PROTOCOL) Server
An FTP server is a piece of software that is running on a computer and uses the File Transfer Protocol to store and share files. Remote computers can connect anonymously, if allowed, or with a user name and password in order to download files from this server using a piece of software called an FTP Client.

FIRMWARE
Firmware is a set of instructions that is embedded in a device at the time of manufacture that allows the device to function. Modern devices often store the firmware in a manner that allows it to be updated periodically.

## 3.0 REFERENCES/RELATED DOCUMENTS

Ontario Software Acquisition Program – http://www.osapac.org

Catholic Curriculum Corporation - *Ethical and Responsible Use of Information and Communication Technology*

## 4.0 RELATED ADMINISTRATIVE PROCEDURES

Workplace Harassment Prevention
Safe Schools - Code of Conduct
API-001 - Responsible Use of Computer Technology and the Internet

## 5.0 RELATED FORMS

Form IT 001, Student Responsible Use of Technology Agreement – Grades JK-3
Form IT 002, Student Responsible Use of Technology Agreement – Grades 4-8
Form IT 003, Student Responsible Use of Technology Agreement – Grades 9-12
Form IT 004, Employee Responsible Use of Technology

**Director of Education:** Glenn Sheculski

**Date Signed:** **July 25, 2013**