Division Finance and Administration	Policy Series 300	Policy # 300.2
Subject Technology	**Replaces**	
Responsible Authority • DIRECTOR OF EDUCATION • ASSISTANT DIRECTOR OF EDUCATION (FINANCE AND ADMINISTRATION) • MANAGER OF INFORMATION SYSTEMS	**Date Approved** ***April 13, 2009***	
	Effective Date ***May 11, 2009***	

300.2(1) Policy Name

Use of Portable Information Storage Devices

300.2(2) Policy Statement

300.2 (2.1) Nova Central School District staff members shall only be permitted to transport and store personal or confidential information [that they have obtained through their official capacity with the district] on board-owned, **encrypted** portable information storage devices (eg. USB Drives, laptops, blackberries) which are authorized by the Manager of Information Systems or his/her designate.

300.2 (2.2) Personal or confidential information shall not be downloaded to personal computers from authorized, encrypted portable information storage devices.

300.2(3) Policy Rationale/Purpose

The Nova Central School District has a responsibility under the *Access to Information and Protection of Privacy Act (ATIPPA)* to take reasonable steps to protect the personal and confidential information it collects from stakeholders. Unencrypted portable storage devices present significant risks for privacy breaches.

This *Use of Portable Information Storage Devices* policy is intended to limit the methods by which personal and confidential information may be temporarily transported or stored.

300.2(4) References

300.2(4.1) Access to Information and Protection of Privacy Act (ATIPPA)
300.2(4.2) Brochure: Using Portable Storage Devices and Laptop Computers - Information for District Staff, Nova Central School District.

300.2(5) Scope

This policy applies to:
300.2(5.1) All authorized users of the Nova Central School District technological resources, including employees, post-secondary students and volunteers.
300.2(5.2) Individuals or agencies contracted by the district to do specified work and who are permitted access to some or all aspects of the district's technological infrastructure and/or information.

300.2(6) Roles and Responsibilities

300.2(6.1) Responsible Division: **Finance and Administration *(Technology)***

6.1.1 The **Assistant Director of Education (Finance and Administration)** shall be responsible for the implementation, monitoring and revision of this policy.
6.1.2 The **Manager of Information Services** or his/her designate shall be responsible for working with district managers and school administrators to:
a) Provide encrypted devices and support in the use of encryption for relevant staff members;
b) Register and assign board-owned, encrypted portable information storage devices.
6.1.3 **School administrators/Managers** are responsible for:
a) Ensuring that staff, volunteers and post-secondary students are aware of this policy;
b) Implementation of the policy in schools and offices;
b) The overall coordination and management of school and office technologies.

300.2(7) Procedures*

N/a

300.2(8) Definitions

300.1(8.1) **Personal Information**
The *Access to Information and Protection of Privacy Act (ATIPPA)* defines personal information as information about an identifiable individual, including:

8.1.1 Name, address and telephone number;
8.1.2 Race, national/ethnic origin, colour, religious or political beliefs or associations;
8.1.3 Age, sex, sexual orientation, marital status or family status;
8.1.4 Number, symbol or other identifier;
8.1.5 Fingerprints, blood type or inheritable characteristics;
8.1.6 Health care status or history;
8.1.7 Educational/financial/criminal history;
8.1.8 Opinions about that person;
8.1.9 The individual's opinion's or views.

300.2(9) Review

This policy shall be reviewed every two years.

300.2(10) School Policy

Schools and other school district worksites are expected to follow the district policy regarding the use of portable information storage devices.