STEO STUDENT TRANSPORTATION OF EASTERN ONTARIO	**Policy**	**Policy # POL702**
Title **Computer Network Security**		
Section **I.T.**	Approved Date **April 16, 2013**	Revised

Associated Documents: POL701: Electronic Communications Systems Policy; TSP701: Electronic Communications System Procedure; TSP702: Computer Network Security Procedure

1.0 PURPOSE

To ensure the appropriate safeguarding, integrity, and availability of physical assets and information stored, processed, or transmitted electronically by STEO.

2.1 DEFINITIONS

In this policy:

(a) **information** is defined as all information holdings that are stored, transmitted, or processed electronically by STEO staff;

(b) **physical assets** are defined as the information technology infrastructure such as computers, software applications, network wiring, encryption devices, etc. used in the processing, storage, and transmittal of information.

3.0 POLICY

3.1 All information at STEO, in whatever form, stored on any media, is an asset and the property of STEO. Similarly, physical assets owned and utilized in the processing of this information are the property of STEO.

3.2 GM, managers and supervisors are accountable for safeguarding information and physical assets under their control. All employees are responsible for the protection of these assets from unauthorized use, modification, disclosure or destruction (whether accidental or intentional) and for maintaining the integrity of these assets and their availability to others as required in the performance of their duties.

3.3 Information and physical assets shall be classified as to their value, sensitivity, integrity, availability and accountability requirements. In addition, information and physical assets shall be safeguarded according to procedures which include their classification and assessment of related risks.

3.4 Access to sensitive information and assets is restricted to those whose duties require such access.

3.5 All staff members are responsible for monitoring and enforcing compliance with this policy within the scope of their duties and responsibilities. Violations or suspected violations of these responsibilities must be reported immediately to the appropriate superintendent, principal or manager/supervisor. Persons found to be in violation of this policy may be subject to immediate disciplinary action up to and including termination of employment. Legal action and/or referral of the matter to law enforcement agencies shall be considered depending on the severity of the violation, the real or potential loss to STEO, or breach of confidentiality.

4.0 REFERENCE DOCUMENTS

The Education Act, 1998, ss. 170, 171