OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

**PROCEDURE PR.564.IT**

**TITLE: COMPUTER NETWORK SECURITY**

**Date issued: February 1999**
**Last revised:**
**Authorization: Senior Staff: 06 January 1999**

## 1.0 OBJECTIVE

To provide guidelines that will ensure the appropriate safeguarding, integrity, and availability of physical assets and information stored, processed, or transmitted electronically by the Ottawa-Carleton District School Board.

## 2.0 DEFINITIONS

In this procedure:

2.1 **Information** is defined as all information holdings that are stored, transmitted, or processed electronically by Ottawa-Carleton District School Board staff and students.

2.2 **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.

2.3 **Sensitive information** is information whose unauthorized disclosure could compromise or reasonably be expected to cause injury to the interests of the OCDSB or individuals within or associated with the OCDSB.

## 3.0 PROCEDURES

3.1 Security Structure

a) The Business/Learning Technologies Department is responsible for developing, implementing, maintaining, co-ordinating and monitoring a security program consistent with Board policy P.074.IT: Computer Network Security. These responsibilities include, but are not limited to:

(i) developing, approving and issuing particular technical standards and guidelines on computer network security;

(ii) providing advice and guidance on the planning, acquisition, installation and use of security related systems;

(iii) conducting periodic risk reviews and providing advice on threat and risk assessments as required;
(iv) evaluating security aspects of products and systems;
(v) providing specialized training on security;
(vi) providing assistance with investigations related to security issues.

b) Superintendents, principals and managers/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. These responsibilities include, but are not limited to:
(i) protecting personal and group account passwords;
(ii) using authorized workstation access tools such as *AtEase*;
(iii) performing regular backups using authorized tools;
(iv) logging off servers and networks after use;
(v) taking reasonable precautions (i.e., security cables, storing equipment in locked rooms, etc.) to secure physical assets;
(vi) using legal copies of software;
(vii) adhering to copyright legislation;
(viii) refraining from accessing the Internet or any other network through unauthorized connections;
(ix) reporting any unauthorized use of OCDSB information or physical assets.

3.2 Classification and Risk Management of Information and Physical Assets

a) Information and physical assets will be classified and safeguarded as to their value, sensitivity, integrity, availability and accountability requirements. The following categories of information are currently in use:
(i) special student records (special education and disciplinary actions);
(ii) general student records (including marks, attendance, and reports on specific students);
(iii) Board budget;
(iv) non-budgetary financial information;
(v) staff performance reviews;
(vi) pay and benefits;
(vii) employment equity and workers compensation;
(viii) management information (unofficial management correspondence, notes and e-mail);
(ix) human resources information;
(x) physical planning information;
(xi) corporate data (for example Director's Council and Board/Committee minutes, memoranda to trustees, OCENET and co-operative ventures information, staff relations and staffing data);
(xii) program evaluation/board wide test results.

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

c) All schools and departments are required to designate a responsibility centre for ensuring that regular back-ups are performed on all servers using approved software and equipment.

d) Schools and central administrative departments must conduct internal reviews of their compliance with this procedure and of the effectiveness and efficiency of its implementation at least once every five years. The Business/Learning Technologies Department will monitor compliance.

3.3 Personnel Security

a) The Human Resources Department will ensure that superintendents, principals and managers/supervisors conduct a basic reference check on any individual who is appointed or assigned to a position in the OCDSB in which there is access to sensitive information.

b) The Human Resources Department is responsible for notifying the Business/ Learning Technologies Department of any employee resignations/terminations. The Business/Learning Technologies Department is responsible for removing the employee's computer access privileges.

3.4 Access to the Internet and other non-Ottawa-Carleton District School Board Networks

a) The Business/Learning Technologies Department will establish and maintain a network firewall to protect the OCDSB network from external unauthorized access, and control internal access to Internet information and facilities.

b) Unauthorized, private Internet connections from any OCDSB networked workstation (including school/department local and wide area networks) are prohibited. No link should be established between any networked Ottawa-Carleton District School Board workstation or server to any non-Ottawa-Carleton District School Board network or computer unless authorized by Business/Learning Technologies. The Ottawa-Carleton District School Board expressly prohibits staff or students from accessing or disseminating any material that is pornographic, racist or promotes violence.

3.5 Security Awareness and Training

a) Superintendents, principals and managers/supervisors are responsible for ensuring that all staff and students are provided with a computer network security awareness program suitable for their needs.

3.6 Contingency Planning

a) Business/Learning Technologies is responsible for the development of a plan of action to recover information in the central computing environment and OCDSB Wide Area Network in the event of a major security incident. Schools and departments are responsible for the development and implementation of a plan of action to recover information within their jurisdiction.

3.7 Security Breaches and Violations

a) All staff are responsible for monitoring and enforcing compliance with this procedure 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 who will investigate and where warranted, take appropriate administrative or disciplinary action.

b) Persons found to be in violation of this procedure may be subject to immediate disciplinary action up to and including termination of employment.

## 4.0 REFERENCE DOCUMENTS

*The Education Act*, 1998, ss. 170, 171
Board Policy P.074.IT: Computer Network Security
Board Policy P.027.GOV: Corporate Records Management
Board Policy P.049.IT: Electronic Communications Systems
Board Policy P.053.HR: Alleged Harassment/Abuse
Board Procedure PR.516.GOV: Corporate Records Management
Board Procedure PR.672.IT: Electronic Communications Systems
Board Procedure PR.564.IT: Computer Network Security