

DUFFERIN-PEEL CATHOLIC DISTRICT SCHOOL BOARD
BOARD POLICY / REGULATIONS

Board Policy Number: 4.75
Subject: Network Use and Security
Effective Date: (530) July 16, 1996; Revised (066) January 25, 2011

The Dufferin-Peel Catholic District School Board (DPCDSB) has developed a robust, secure, safe, and reliable system-wide network that is pervasive in virtually all areas of the Board. The network is used to provide authorized stakeholders with access to a variety of systems and services. Some examples include employee e-mail, the student information system, the transportation system, the finance system, the human resources and payroll system, the Safe Schools application, the business intelligence system, published and virtualized applications for instructional and administrative use, user and shared data, the telephone system, and the Internet. The network facilitates access to resources that can assist Teachers in transforming pedagogy so that they can engage and motivate their students to be active learners in an ambience that is highly conducive to learning. Through the effective use of networked technology, students are encouraged to be well prepared for the global workplace of the 21st century. The School Board's networked resources also facilitate workplace efficiencies for its employees.

At all times, staff and students of the Board will abide by all rules and regulations, including the Catholic Code of Behaviour and the Employee Code of Conduct on the use of network resources. In the spirit of its Mission Statement, DPCDSB's Wide Area Network connects all of its sites together. It must be noted, however, that the School Board does not have control over the information that is accessible on other networks, nor can it erect barriers that completely limit access to the full range of information available. Information available on the Internet may be objectionable in that it may contain matter which is illegal, defamatory, pornographic, inaccurate, or opposed to the Mission Statement of the Board and the Board's vision of students.

Ultimately, parents and guardians, supported by the School Board and its staff, are responsible for setting and conveying the standards that their children should follow.

DPCDSB's network has been designed to allow access to, and promote the use of, a vast amount of information and other resources that are available both within our organization and on the Internet from anywhere in the Board. Remote access for Board employees is also available through DPCDSB's Virtual Private Network (VPN).

The School Board will make every reasonable effort to protect its network from malware infestations and other security breaches and ensure that access to the negative aspects of global communications are limited. To that end, the following regulations have been developed.

REGULATIONS

4.75 NETWORK USE AND SECURITY

The following activities are prohibited on DPCDSB's Network regardless of the method being used to gain access to the network. Users are prohibited from:

- i) engaging in illegal, unethical, or malicious acts;
- ii) intentionally sending files or messages containing programs designed to disrupt other systems and/or data (computer malware);
- iii) intentionally bypassing the Board's Internet Content filter;
- iv) accessing any Board resource without explicit authorization inside or outside of the Board's network (commonly known as hacking);
- v) possessing, using, or transmitting unauthorized material (i.e. copyright protected);
- vi) creating, possessing or distributing unlawful information on any computer system accessed through the Dufferin-Peel Network. This includes pornographic, obscene or other unacceptable / objectionable material;
- vii) sending messages that include profanity, sexual, racial, religious, political opinions, or ethnic slurs or other abuse, threatening or otherwise offensive language;
- viii) sending messages that are not professional and courteous;
- ix) disclosing of personal information contrary to the *Municipal Freedom of Information and Protection of Privacy Act (M-FIPPA)*;
- x) using the network for commercial objectives;
- xi) using the network for Union/Association-related business and/or without the expressed written consent of the Superintendent of Employee Relations/designate;
- xii) connecting devices to the Board's network that are not explicitly approved in writing by the Information and Communication Technology Department (for example, non-Board owned or leased devices, printers, wireless access points, network switches, etc);
- xiii) relocating any of the School Board's networked resources (computers, printers) without following the processes that are put in place by the Information and Communication Technology Department;
- xiv) tampering with or moving the Board's internetworking equipment such as patch panels and network switches;
- xv) disconnecting any of the School Board's resources from the Board's network without expressed authorization from the ICT Department.

Breaches to these regulations are subject to sanctions and/or discipline.

Conditions of Use

Access to DPCDSB's Network is at the user's own risk. The Dufferin-Peel Catholic District School Board makes no warranties, whether expressed or implied, with respect to network services, and it specifically assumes no responsibilities for:

- a) the accuracy or quality of any advice or information obtained by a user from any source accessed via the network;
- b) any costs, liability or damages caused by the use of the network;
- c) any consequences of service interruptions or changes in services, including loss of data, resulting from delays, non-deliveries or mis-deliveries, even if these disruptions arise from circumstances under the control of the Board.

All e-mail residing on the School Board's e-mail system is School Board property and may be subject to further scrutiny, if necessary.

It should be noted that electronic communications via the DPCDSB's Network is not guaranteed to be private. Certain ICT staff has the ability to monitor network traffic, examine electronic communications and monitor the flow of such electronic communications. Employees should be aware that there is to be no reasonable expectation of privacy when using the network.

It is critical to the security of the DPCDSB's Network that all users do their part to safeguard the security precautions in place. Users that can identify a security problem on the network must notify the Information and Communication Technology Department.

Users are prohibited from:

- a) demonstrating a security problem to other users;
- b) using another person's user account;
- c) sharing user accounts and passwords.

.....