Dufferin-Peel Catholic District School Board

DUFFERIN-PEEL CATHOLIC DISTRICT SCHOOL BOARD POLICY	
POLICY NUMBER:	P-5004
SUBJECT:	Acceptable Network Use and Security
REFERENCE:	P-1009 Harassment and Discrimination P-0002 Catholic Code of Conduct GAP2012 Catholic Code of Conduct GAP5013 Employee Workplace Conduct (Including Workplace Harassment)
EFFECTIVE DATE:	July 16, 1996
REVISED DATE:	January 25, 2011; April 20, 2021; February 23, 2022; October 25, 2022; April 29, 2025

"But you, O Lord, are a shield around me, my glory, and the one who lifts up my head."
Psalm 3:3

1. 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 DPCDSB. The network provides 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.

2. The DPCDSB network infrastructure facilitates access to resources that assist teachers in transforming pedagogy to engage and motivate their students to be active learners in an environment that is highly conducive to learning. Through the effective use of networked technology, students are well prepared for the global workplace of the 21st century. DPCDSB's networked resources also facilitate workplace efficiencies for its employees.

3. At all times, use of network resources by staff and students of DPCDSB will be in accordance with applicable polices, including *P-0002 Catholic Code of Conduct*, *General Administrative Procedure (GAP) GAP2012 Catholic Code of Conduct, P-1009 Harassment and Discrimination*, and *GAP5013 Employee Workplace Conduct (Including Workplace Harassment)*, each as may be amended or replaced.

4. DPCDSB's Wide Area Network (WAN) connects all its sites together. However, DPCDSB does not have control over the information that is accessible on other networks, nor can DPCDSB 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 content that is illegal, defamatory, pornographic, inaccurate, or opposed to DPCDSB's mission and vision. Parents and guardians, supported by DPCDSB and its staff, are responsible for setting and conveying the standards that their children should follow.

5. DPCDSB's network allows access to and promotes the use of a vast amount of information and other resources that are available both within DPCDSB and on the Internet, from anywhere in DPCDSB. Remote access for DPCDSB employees is also available through DPCDSB's Virtual Private Network (VPN).

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

7. 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:

   - Engaging in illegal, unethical, or malicious acts.
   - Intentionally sending files or messages containing programs designed to disrupt other systems and/or data (computer malware).
   - Accessing, or attempting to access, any DPCDSB resource without explicit authorization inside or outside of DPCDSB's network (commonly known as hacking).
   - Possessing, using, or transmitting unauthorized material (i.e., copyright protected).
   - Creating, possessing, or distributing unlawful information on any computer system accessed through the DPCDSB network, including material that is pornographic, obscene, or otherwise unacceptable/objectionable.
   - Sending messages that include: hate speech, political opinions, profanity, sexual, racist, religious, or ethnic slurs, or other abusive, threatening, or otherwise offensive language.
   - Sending messages that are not professional and courteous.
   - Disclosing of personal information contrary to the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and other applicable privacy laws.
   - Using the network for commercial objectives.
   - Using the network for Union/Association-related business and/or without the expressed written consent of the Superintendent of Employee Relations/designate.
   - Connecting wired devices to DPCDSB's network that are not explicitly approved in writing by the Information and Communication Technology (ICT) Department (e.g., non-DPCDSB owned or leased devices, printers, wireless access points, network switches, etc.).
   - Relocating any of DPCDSB's networked resources (e.g., computers, printers) without following the processes that are put in place by the ICT Department.
   - Tampering with or moving DPCDSB's internetworking and/or telecom equipment such as patch panels, network switches, and wireless equipment.
   - Disconnecting any of DPCDSB's resources from DPCDSB's network without express authorization from the ICT Department.
   - Disseminating or storing of destructive or malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, or other self-replicating code).

8. Individuals who breach this policy may be subject to discipline.

9. Access to DPCDSB's network is at the user's own risk. DPCDSB makes no warranties, whether expressed or implied, with respect to network services, and it specifically assumes no responsibility for:

   - The accuracy or quality of any advice or information obtained by a user from any source accessed via the network.
   - Any costs, liability, or damages caused by using the network.

- 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 DPCDSB.

10. All e-mail travelling through DPCDSB's e-mail system is DPCDSB property and may be subject to further scrutiny.

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

12. Users are prohibited from:

    - Deliberate, unauthorized access to information, facilities, or services accessible through the DPCDSB's infrastructure.
    - Willfully bypassing or subverting DPCDSB's physical, logical, or procedural safeguards such as firewalls, web-filtering software, or other access controls.
    - Revealing account passwords to others or allowing someone else to access or use the user's account. This prohibition includes, but is not limited to, family and other household members when work is done at home.
    - Using another user's password, secure token, digital certificates, or any other identifier to engage in any activity in violation of applicable laws.

13. It is critical to the security of the DPCDSB's network that all users do their part to safeguard the security precautions in place. If a security problem is identified on the network, the user must immediately notify the ICT Department.