

GAP GENERAL ADMINISTRATIVE PROCEDURE

SECTION:	500 – SCHOOL ORGANIZATION AND MANAGEMENT
GAP NUMBER:	541.00
SUBJECT:	Personal Electronic Devices (PEDs) on School and DPCDSB Premises
REFERENCE:	<p>Board Policies: 6.02: Records and Information Management 8.12: Personal Electronic Devices 4.14: Freedom of Information and Protection of Privacy; 4.75: Acceptable Network Use and Security; 9.01: Catholic Code of Conduct; 9.02: Bullying Awareness, Prevention, and Intervention; 9.03: Progressive Discipline</p> <p>General Administrative Procedures: 312.08 – Municipal Freedom of Information and Protection of Privacy – Student Personal Information 312.10 – Privacy Breach: Best Practices for Responding 530.00 – Catholic Code of Conduct; 540.00 – Document Retention Schedule 551.00 – Bullying Awareness, Prevention, and Intervention 552.00 – Progressive Discipline</p>
EFFECTIVE:	January 30, 2007
REVIEWED/AMENDED	December 1, 2014; February 23, 2022

*“An educated person knows many things.”
Sirach 34:9*

1. INTRODUCTION AND PURPOSE

- 1.1. This General Administrative Procedure (GAP) applies to electronic devices not owned by the Dufferin-Peel Catholic District School Board (DPCDSB), but which are used on DPCDSB premises and/or at DPCDSB-sanctioned events for educational purposes.
- 1.2. DPCDSB school principals will align the use of personal electronic devices (PEDs) by students to DPCDSB policies and procedures. In the event of a conflict between or among policies or procedures, the more restrictive use policy/procedure shall govern.
- 1.3. PEDs are personal electronic devices that include, but are not limited to laptops, tablets, cell phones, smartphones and wearable technology

- 1.4. With a view to achieving the Ontario Catholic School Graduate Expectations, aligned to the Multi-Year Strategic Plan (MYSP) and annual operational plan, DPCDSB is committed to supporting appropriate access to technology for all in a Christ-centred environment that is safe, caring, and inclusive. DPCDSB supports the dignity of all through the *Catholic Code of Conduct*, which outlines appropriate behaviour, including the use of PEDs.
- 1.5. Student use of PEDs on DPCDSB premises and/or at DPCDSB-sanctioned events shall only occur under the direction of staff and only with parent/guardian permission (unless students are aged 18 years or are aged 16 or 17 years and have withdrawn from parental control), as agreed to by signing a *General Form 337: Personal Electronic Device Used With WI-FI Network Student Agreement*.
- 1.6. Access and use of technology and its aligned infrastructure, including wireless network supports, are intended to support student well-being and achievement, to assist students and staff who support them, and to facilitate the business and daily operations of DPCDSB.

2. CREATING A POSITIVE CATHOLIC CLIMATE

- 2.1. DPCDSB acknowledges that the dignity of the human person, as promoted by the Catholic Church, may be compromised by the potential for invasion of personal privacy made possible by the inappropriate use of PEDs on school or other DPCDSB premises.
- 2.2. DPCDSB recognizes that the unregulated use of PEDs may pose a risk to the individual safety of students, staff, and/or visitors in DPCDSB schools or other sites. In some cases, unregulated use of PEDs may facilitate illegal activities in the school environment or workplace, or during school- or DPCDSB-sanctioned activities.
- 2.3. DPCDSB understands that its employees, particularly those in frontline roles, are religious and moral role models for the students placed under their care. In this light, all DPCDSB employees are expected to regulate their use of PEDs in accordance with the requirements, procedures, and notices contained in this GAP.
- 2.4. DPCDSB regulates the use of PEDs on school or other DPCDSB premises by prohibiting the following uses:
 - The use of a PED that compromises the academic integrity of the school or individuals within the school.
 - The use of a PED that interferes with or disrupts the academic day or the teaching and learning environment.
 - The use of a PED that violates a person's reasonable expectation of privacy.
 - The use of a PED that compromises personal and/or school/workplace safety.
 - The use of a PED that facilitates the commission of a crime.
 - Any other use of a PED which the school principal or DPCDSB deems compromises or interferes with school/site security, personal safety, individual privacy, or academic integrity.

3. REGISTRATION OF PEDS

- 3.1. Students and their parent/guardians (unless students are aged 18 years or are aged 16 or 17 years and have withdrawn from parental control) must sign and return *General Form 337: Personal Electronic Device Used With WI-FI Network Student Agreement* before access is granted to DPCDSB wireless network services.
- 3.2. Students and staff connecting their PEDs to the DPCDSB wireless network must provide their valid DPCDSB student or employee credentials (i.e., student or employee number, as applicable, and password).
- 3.3. Students and staff connecting their PEDs to the DPCDSB wireless network must not share their DPCDSB account credentials.

4. SCOPE

- 4.1. The owner of the PED (e.g., student, adult student, parent and/or guardian, or staff member) is responsible for their own equipment, including the hardware, installation, maintenance, security and configuration of software or settings.
- 4.2. DPCDSB will not support or maintain PEDs. DPCDSB will not be responsible for any cost incurred by using PEDs.
- 4.3. PEDs that are lost, stolen, or damaged are not the responsibility of DPCDSB.
- 4.4. Anyone choosing to use the DPCDSB wireless network is doing so of their own volition and risk.
- 4.5. Wireless network access is a privilege, not a right.
- 4.6. There is no reasonable expectation of privacy for any individual using the DPCDSB wireless network.
- 4.7. PEDs can be connected to the DPCDSB network via wireless technology, but connection via wire is prohibited.
- 4.8. A record is a document, regardless of physical format or characteristics, that memorializes and provides objective evidence of activities performed, events elapsed, results achieved, or statements made in the course of the organization's daily activities. Downloading of any DPCDSB records, data, or intellectual property to a PED that is connected to the DPCDSB wireless network is prohibited.
- 4.9. Storage of DPCDSB records, data, or intellectual property on PEDs is prohibited.
- 4.10. Where reasonable grounds exist, DPCDSB reserves the right to monitor the use of PEDs on school premises and/or during school related activities.

- 4.11. DPCDSB further reserves the right to terminate or suspend the wireless network access of a particular user and/or device, if deemed that such user or device compromises the integrity of the network or conflicts with the *Catholic Code of Conduct* and other DPCDSB policies and procedures, in addition to other consequences as appropriate.

5. AUTHORIZED SERVICE RESTRICTIONS

- 5.1. It is the responsibility of any student (and/or the parent/guardian) or staff member who uses a PED to address normal and reasonable security measures, such as maintaining up-to-date anti-virus protection and security patches for software for their own protection and for those with whom they share the wireless network.

6. ACCESS AND DISCLOSURE

- 6.1. DPCDSB will establish audit trails, which may be accessed, reproduced, and used without notice or permission of a PED owner. The student (and/or parent/guardian) or staff member agrees to and accepts that their access and/or network activity may be monitored to record dates, times, duration of access, or other relevant information, in order to identify usage patterns, security issues, and for any other reason deemed necessary by DPCDSB.
- 6.2. Where reasonable grounds exist, such audit trails will be able to track the attachment of student or employee information and their external device to the wireless network, and the resulting reports may be used for investigation of possible breaches and/or misuse. Such investigation may result in disciplinary action, up to and including expulsion for students and termination of employment with DPCDSB for staff.
- 6.3. DPCDSB reserves the right to determine what type of equipment can be connected to its wireless network. DPCDSB also reserves the right to refuse the ability to connect PEDs to the DPCDSB wireless network if such equipment puts DPCDSB's systems, data, users, and/or clients at risk, or if behaviour is counter to policy, procedures, codes of conduct, or to the interests of DPCDSB.
- 6.4. DPCDSB will manage security policies, wireless network, application, and data access centrally using the technology solutions it deems suitable.
 - 6.4.1. Students must comply with the terms and conditions of *General Form 337: Personal Electronic Device Used With WI-FI Network Student Agreement*. Any attempt to contravene or bypass this process is in violation of existing DPCDSB policies and may be subject to disciplinary action.
 - 6.4.2. Staff must comply with the terms and conditions of *Policy 8.12: Personal Electronic Devices*, this GAP, the *Catholic Code of Conduct*, and all DPCDSB policies and procedures, in addition to any agreements and/or notices provided to staff as agreed upon or required as a condition of employment.

7. GENERAL

- 7.1. References to DPCDSB policies, procedures, forms, or other documents and to applicable laws includes as they are amended or replaced.