Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure **Personal Device Network Access**	Administrative Procedure Number **314**
Directional Policy **300 - Student Achievement and Well Being**	

Title of Administrative Procedure:

Personal Device Network Access

Date Approved:

June 25, 2024

Projected Review Date:

2029

Directional Policy Alignment:

This Administrative Procedure aligns with the purpose of the Student Achievement and Well Being Directional Policy by supporting a learning environment that is anchored in the teachings of the Gospel, Catholic Social Teachings, and the Catholic Graduate Expectations in the context of personal devices used in our classrooms.

Alignment with Multi-Year Strategic Plan:

The Personal Device Administrative Procedure supports our Vision for achieving Excellence in Catholic Education by ensuring the Board has clearly outlined the requirement for the acceptable use of personal devices. The board is committed to creating a shared understanding and a systematic approach to the implementation of effective and responsible use of our technology systems. Technology is everywhere in our lives. This necessitates a collective effort and active engagement of our entire community, including students and parents, to ensure that technology use helps further our mission and strategic priorities.

PVNCCDSB Board Vision, Mission and Strategic Priorities

Action Required:

The Peterborough Victoria Northumberland and Clarington Catholic District School Board (the "Board") is committed to enabling students and employees access to the Board's network for education related purposes and in a manner that is not detrimental or harmful to the interests of others. The Board will provide this access while maintaining the security and effectiveness of the Board's network. The Board will provide network access to Personal Devices to further the educational goals of the Board and will at the same time implement controls and processes to protect the integrity of other network connected devices.

The Board will, from time to time and without prior notice to the user, access and/or monitor the Board's Electronic Information Systems. Principals will be informed of any serious infraction of the Acceptable Use of Technology Policies. Disciplinary actions of a user will be handled in accordance with the discipline policies of the Board and the school.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment with the Student Achievement and Well Being Directional Policy.
- Reviewing the Personal Device Administrative Procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Designating resources for ensuring the implementation and compliance with this Administrative Procedure.

Superintendents of Schools and System Portfolios are responsible for:

- Supporting implementation of this Administrative Procedure.
- Promoting a culture of positive digital citizenship that reinforces our Catholic virtues

Superintendent of Information Technology (or designate) is responsible for:

- Monitoring usage of the board's network systems.

- Ensuring the use of Personal Devices does not impact the integrity of the Board's technology systems.
- Working with the fire wall providers, to ensure that social media can not be accessed by students through the PVNC Catholic networks.
- Determining, at the Board's discretion, the network access provided for Personal Devices:
    - Suitability of any personal device to be connected to the BYOD network
    - Resources or access restrictions when a device is connected
    - Revoking network access from personal devices
- Monitoring the use of Personal Devices on the Board's network which may include:
    - Monitoring of network activity
    - Filtering and/or throttling traffic to the Device
    - Logging network activity, including internet access, to and from the Device
    - Performing system scans to evaluate the security level of the Device including, but not limited to, the update status of Antivirus, Spyware, and system components.
    - Performing system scans to determine compliance with the Board's Acceptable Use Policies and applicable laws.
    - Authorizing a physical inspection of the Device if deemed necessary.
- Providing digital citizenship and internet safety resources for staff and students.
- Overseeing network access compliance for personal devices with legal and ministry directives

Principals and Vice-Principals are responsible for:

- Ensuring that students or employees using a personal network device (the Device) have completed the Acceptable Use of Technology form and will maintain a copy of the form in the school's files. An electronic acknowledgement of the agreement may also serve as the official record in lieu of a paper copy.
- Ensuring that the provided digital citizenship training is completed by their staff and students.
- Ensuring the use of a personal network device during instructional time is permitted under the following circumstances:
    - for educational purposes, as directed by an educator
    - for health and medical purposes
    - to support special education needs
- Ensuring student devices are out of sight and set to off or silent for grades K-6 for the entire instructional day, while grade 7-12 student devices must be out of sight and set to off or silent unless they have explicit direction from the teacher.

- Sharing reminders with students they are not to be accessing social media during the school day.
- Ensuring students and staff only connect personal devices to the permitted BYOD wireless network.

Educators are responsible for:

- Ensuring the use of a personal network device during instructional time is permitted under the following circumstances:
    - for educational purposes, as directed by an educator (grades 7-12 only)
    - for health and medical purposes
    - to support special education needs
- Providing students with digital citizenship instruction as outlined in the Digital Privacy Scope and Sequence per Administrative Procedure 322 - Digital Privacy.
- Ensuring that the guidelines, resources and frameworks developed for board use of digital tools are followed.
- Advising students that the Board will from time to time and without prior notice to the student, access and/or monitor the Board's Electronic Information Systems including those Personal Network Devices used to access the Board's systems.
- Ensuring student devices are out of sight and set to off or silent for grades K-6 for the entire instructional day, while grade 7-12 student devices must be out of sight and set to off or silent unless they have explicit direction from the teacher.
- Sharing reminders with students they are not to be accessing social media during the school day.
- Ensuring students only connect personal devices to the permitted BYOD wireless network.

Staff are responsible for:

- Ensuring that the guidelines, resources and frameworks developed for board use of digital tools are followed.
- Completing on an annual basis the Employee Acceptable Use of Technology Agreement.
- Ensuring they do not use their Personal Device to store "personal information" as defined in the Municipal Freedom of Information and Protection of Privacy Act.
- Ensuring student devices are out of sight and set to off or silent for grades K-6 for the entire instructional day, while grade 7-12 student devices must be out of sight and set to off or silent unless they have explicit direction from the teacher.
- Sharing reminders with students they are not to be accessing social media during the school day.

- Ensuring personal devices are only to connect to the permitted BYOD wireless network.

Students are responsible for:

- Using available technology to further their educational goals and promote Catholic teaching and at the discretion of an Educator.
- Reading, acknowledging and following the Student Acceptable Use of Technology Agreement appropriate for their grade on an annual basis.
- Ensuring their use of a personal network device during instructional time adheres to PPM 128, thus:
    - Students in grades K-6 must have their personal network devices and personal mobile devices are out of sight, turned off or set to silent for the entire instructional day;
    - Students in grades 7-12 without the explicit permission of the Teacher, must have their personal network devices and personal mobile devices are out of sight, turned off or set to silent for instructional time;
- Ensuring personal devices are only to connect to the permitted BYOD wireless network.

All users of Personal Network Devices are responsible for:

- Ensuring their Personal Device is updated with software and/or firmware updates as recommended by the manufacturer and that, where applicable, the Device has antivirus software installed and that the definitions for the software are up to date.
- Ensuring personal devices are only connected to the permitted BYOD wireless network.
- Ensuring that the personal device is on the approved personal device list.

Parents are responsible for:

- Reading, supporting, and acknowledging by signing the Student Acceptable Use of Technology Agreement appropriate for their child's grade on an annual basis.

Approved Personal Devices:

- Cellphones
- Tablets
- Laptops (students and supply staff only)
- Medical Devices

Prohibited Personal Devices:

- Network Appliances (modems, routers, switches, network attached storage etc.)
- Desktop computers
- Gaming systems
- Smart Devices
- Televisions

Exclusions:

Under special circumstances, the board may approve the use of prohibited personal devices. Use of prohibited devices requires explicit permission from the Superintendent of Information Technology.

Progress Indicators:

- Yearly completion of Student Acceptable Use of Technology forms by students and parents.
- Student access to Digital Citizenship resources.

Definitions:

- **Board Managed Device** – This refers to any electronic device owned, distributed, and maintained by the Board. Examples include laptops, tablets, desktops, as well as audio-visual equipment like TVs, projectors, and smartboards.
- **Digital Tools** - Electronic tools that are used to help deliver instruction or for other classroom purposes. A movie maker app is an example of a digital tool that can be used to help students create a movie to help explain a concept they are learning.
- **Educator** - refers to teachers regulated under the Ontario College of Teachers Act, 1996, and early childhood educators regulated under the Early Childhood Educators Act, 2007 per PPM 128.
- **Firmware** – A set of instructions that is embedded in a device at the time of manufacture that allows the device to function. Modern devices often store the firmware in a manner that allows it to be updated periodically.
- **FTP Server** - An FTP Server is a piece of software that is running on a computer and uses the File Transfer Protocol to store and share files. Remote computers can connect anonymously, if allowed, or with a username and password in order to download files from this server using a piece of software called a FTP Client.
- **Gaming System** – An electronic device or console specifically designed for playing video games. These devices typically connect to a TV or monitor and

provide powerful graphics and processing capabilities for immersive gaming experiences. Examples include Sony Playstation, Xbox, Nintendo Switch etc.

- **Medical Device** – Any instrument, apparatus, implant, material, or other article intended for use in the diagnosis, prevention, monitoring, treatment, or alleviation of disease, or to affect the structure or function of the body for health or other therapeutic purposes. Examples include Medical monitoring devices, therapeutic devices, assist devices.
- **Multi-radio device** – A network device which employs more than one radio to connect to multiple networks. Some cellular telephones will allow users to choose whether they connect to a cellular network or to a computer network in order to access the internet.
- **Network Device** – Electronic equipment designed to connect devices to a computer network and facilitate communication between them. Examples include routers, switches, modems, hubs, and network attached storage.
- **Nexus** - The umbrella for “school behaviour” includes matters which fall under the category of “nexus”. Nexus means “relevant”. The student’s behavior off school property and/or outside the school day may have a relevant and related impact on the safety and well-being of the school community.
- **Personal Mobile Device** is a device that is both portable and capable of collecting, storing, transmitting or processing electronic data or images. Examples include laptops or tablet PCs, personal digital assistants (PDAs), smart watches and “smart” phones. This definition also includes storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to the device.
- **Personal Device** – A personal device is any electronic equipment you own and manage, like laptops, tablets, or smartphones.
- **Smart Device** – An electronic device with built-in computing capabilities and internet connectivity, allowing interaction with users and other devices. These devices can often be controlled remotely and may collect and share data. Examples include Google Home, Alexa, smart wearables, smart speakers, smart displays etc.
- **Technology** - all forms of technology used to create, store, exchange, and use digital information in its various forms (data, audio, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).
- **Web Server** – A computer program that serves the requested files which form web pages to the client's browser

References:

- Catholic Curriculum Corporation - Ethical and Responsible Use of Information and Communication Technology
- Bill 13, Accepting Schools Act, 2012
- Learning Technologies BYOD Guidelines and Supports
- Learning Technologies Digital Privacy Scope and Sequence
- Policy/Program Memorandum (PPM) 128 “The Provincial Code of Conduct and School Board Codes of Conduct”
- Board Code of Conduct
- Student Achievement and Well Being Directional Policy - 300
- Student Acceptable Use of Technology - AP 313
- Employee Acceptable Use of Technology - AP 511