Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure **Cybersecurity**	Administrative Procedure Number **602**
Directional Policy **Stewardship of Resources**	

Title of Administrative Procedure:

Cybersecurity

Date Approved:

1 November 2022

Projected Review Date:

2027

Directional Policy Alignment:

This Administrative Procedure aligns with the Stewardship of Resources Directional Policy – 600 by recognizing digital information, information systems, education technology and internet connectivity are integral parts of the board’s technology systems. They are essential in day-to-day operations, administrative functions, facilities management, and they help to enhance teaching and learning in school and during remote learning. As such, the board aims to take appropriate action to manage cyber risks and mitigate current and evolving cyber threats.

Alignment with Multi-Year Strategic Plan:

This Administrative Procedure supports the “Expanding Technology” priority by ensuring the technology used to facilitate ongoing learning is safe and secure. It also supports the “Maximizing Resources” priority by documenting, prioritizing and addressing corporate risk related to cybersecurity.

PVNCCDSB Board Vision, Mission and Strategic Priorities

Action Required:

Every individual in the board has a responsibility to protect board IT resources they use or are otherwise within their control. These responsibilities vary based on the functional role of the individual. Depending on those functions, some individuals may have more than one role. Responsibility for board cybersecurity is delegated by the Director of Education to Board Superintendents and their departments and staff.

1.0 General Principles

1.1. Information and information systems are critical school board assets, like physical infrastructure and financial resources, and shall be safeguarded deliberately, appropriately and consistently throughout their life cycle.

1.2. Cybersecurity shall be provided in a manner that serves the security and safety of students and staff while adhering to legislative requirements.

1.3. Appropriate safeguards shall be in place to ensure the protection of students' and staff privacy and their safety online. The effort taken to apply those safeguards shall be proportionate to the possible harm or injury that could result if confidentiality, integrity and availability are not assured.

1.4. All students and staff shall be informed of safe, responsible and ethical online behaviours and understand their accountability for the protection of information that is received, created, or maintained on behalf of the board.

1.5. The Board, schools and all staff have a duty of care to take reasonable steps to protect students from harm encountered within the online learning environment.

1.6. The board aims to facilitate secure, safe, responsible and respectful use of technology as is further defined in the board's acceptable use Administrative Procedures for Staff and Students (AUT) to support teaching and learning and prepare students for the risks and opportunities of the digital world, to thrive safely online, and become good digital citizens.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment with the Stewardship of Resources Directional Policy

- Reviewing the Cybersecurity Administrative Procedure as part of its regular policy and procedures review cycle.

The Director of Education is responsible for:

- Ensuring compliance with the Cybersecurity Administrative Procedure and the Stewardship of Resources Directional Policy.
- Designating resources to implement this Administrative Procedure.

Superintendent of Business is responsible for:

- Alignment of this Administrative Procedure with the Board’s overall Governance, Risk and Compliance efforts.
- Alignment of this Administrative Procedure with the Board’s overall Business Continuity Program.

Manager of Information Technology is responsible for:

- Developing and implementing the Cybersecurity Handbook.
- Establishing and maintaining a multi-year plan for implementing and improving cybersecurity in the board as part of the Board’s overall technology strategy.
- Developing and implementing training in Cybersecurity appropriate for the level of access provided for staff.
- Supporting the continuing improvement of the Board’s Cybersecurity through regular assessments and testing.
- Working collaboratively with internal and external audit as required/appropriate.

Superintendents of Schools and System Portfolios, Principals, Managers & Supervisors are responsible for:

- Ensuring all school and department technology is compliant with the Cybersecurity Administrative Procedure and the Cybersecurity Handbook.

Staff are responsible for:

- Complying with the Board’s Employee Acceptable Use of Technology AP and other technology related guidance as issued from the Board’s IT Services.
- Alerting their immediate supervisor upon learning of misuse or compromise of technology systems.

Students are responsible for:

- Complying with the Board’s Student Acceptable Use of Technology AP and other technology related guidance as issued from the Board’s IT Services.
- Alerting a school staff member upon learning of misuse or compromise of technology systems.

Progress Indicators:

- Cyber Assessment status and improvement (e.g. Centre for Internet Security Critical Security Controls Assessment)
- Third Party Security Assessments (e.g. Ontario School Boards' Insurance Exchange)
- Completion of Cybersecurity and Information Protection training through the Board's online employee training tool.

Definitions:

Cybersecurity: The systems, technologies, processes, governing policies and human activity that an organization uses to safeguard its digital assets.

Data Protection: A set of strategies and processes used to ensure the privacy, availability, and integrity of your data.

References:

- Education Act
- AP 313 - Student Acceptable Use of Technology
- AP 314 - Personal Network Devices
- AP 322 - Student Digital Privacy
- AP 511 - Employee Acceptable Use of Board Technology
- AP 615 - Emergency Management and Business Continuity Program
- Centre for Internet Security Critical Security Controls
- Policy 600 - Stewardship of Resources
- Student Digital Learning Scope and Sequence
- Message of His Holiness Pope Francis for World Communications Day, January 24, 2018
- Catholic Curriculum Corporation - Ethical and Responsible Use of Information and Communication Technology