Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

Agenda

POLICY DEVELOPMENT COMMITTEE MEETING

Wednesday, May 13, 2020
6:30 – 8:30 p.m.
VIRTUAL GOOGLE MEETING

Chairperson: Emmanuel Pinto

Trustees who are unable to attend are asked to please notify
Andrea Bradley, Administrative Assistant
abradley@pvnccdsb.on.ca

A. Call to Order:

1. Opening Prayer, Kevin MacKenzie.
2. We acknowledge that we are meeting on the traditional territory of the Mississauga Anishinaabe.
3. Approval of Agenda.
4. Declarations of Conflicts of Interest.
5. Approval of the Draft Minutes of the Policy Committee Meeting held on February 4, 2020. Page 3
6. Business Arising from the Minutes.

B. Presentations / Recommended Actions:

1. R.A.: Draft Administrative Procedure – New #1209 Page 9
   Privacy Breach Response
   Galen Eagle, Communications Manager

2. R.A.: Draft Administrative Procedure – New #314 (Old #904) Page 24
   Personal Network Devices
   Pepe Garieri, Superintendent of Learning / P/J Program / Information Technology
   Sean Heuchert, Information Technology Services Manager

3. R.A.: Remove Policies and Administrative Procedure – Page 31
   #602 – (Old Policy #105)
   School Sites – Operating Budget Surplus
   #603 – (Old Policy and Administrative Procedure #106)
   Alternative Arrangements for School Facilities
   Isabel Grace, Superintendent of Business and Finance

4. R.A.: Draft Administrative Procedure – New #902 (Old #411) Page 32
   Visitors to Schools
   Tim Moloney, Superintendent of Learning / Student Success

5. R.A.: Draft Administrative Procedure – New #901 (Old #814) Page 37
   Safe Arrivals
   Tim Moloney, Superintendent of Learning / Student Success

C. Information Items:

D. Next Meeting:

1. September 2020
   6:30 – 8:30 p.m.

E. Conclusion:

1. Closing Prayer, Linda Ainsworth.
2. Adjournment.

2020-PD-1

Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

Minutes

THE MINUTES OF THE POLICY DEVELOPMENT COMMITTEE MEETING held on Tuesday, February 4, 2020 at 6:30 p.m. in the Boardroom, 1355 Lansdowne Street West, Peterborough.

PRESENT

Trustees: Mmes. Linda Ainsworth, Eveline Fisher (Senior Student Trustee), Helen McCarthy, Michelle Griepsma.

Messrs. David Bernier, Braden Leal, Kevin MacKenzie, Emmanuel Pinto (Committee Chairperson).

Administration: Mmes. Joan Carragher, Laurie Corrigan, Isabel Grace, Dawn Michie.

Messrs. Pepe Garieri, Timothy Moloney, Michael Nasello.

Guests: Mr. Sean Heuchert, Information Technology Services Manager.

Regrets: Mr. Josh Hill (Junior Student Trustee).

Recorder: Mrs. Andrea Bradley.

A. **Call to Order**:

Emmanuel Pinto called the meeting to order.

1. Opening Prayer.

The Committee Chairperson, Emmanuel Pinto, called the meeting to order at 6:30 p.m. and asked Michelle Griepsma to lead the Opening Prayer.

2. Emmanuel Pinto, Committee Chairperson, acknowledged that the Policy Development Committee Meeting was taking place on the traditional territory of the Mississauga Anishinaabe.

3. Approval of the Agenda.

MOTION: Moved by Braden Leal, seconded by Linda Ainsworth, that the Policy Development Committee Agenda be accepted.

Carried

4. Declarations of Conflicts of Interest.

5. Approval of the Minutes of the Policy Development Committee Meeting held on November 19, 2019.

MOTION: Moved by Michelle Griepsma, seconded by Braden Leal, that the Minutes of the Policy Development Committee Meeting held on November 19, 2019, be approved.

Carried.

6. Business Arising from the Minutes.

Dawn Michie, Superintendent of Learning / I/S Program / Faith and Equity, shared with Policy Development Committee, a letter announcing her retirement effective April 30, 2020 after 22 years of service in a variety of positions with the PVNCCDSB. Trustees congratulated Dawn on her retirement and wished her well in her future endeavours. Michael Nasello, Director of Education, also congratulated Dawn on behalf of the Senior Administration Team.

B. Recommended Actions/Presentations:

1. R.A.: Draft Administrative Procedure – New #322

Student Digital Privacy

Sean Heuchert, Information Technology Services Manager, presented new draft Administrative Procedure – ***#322 – Student Digital Privacy*** to the Policy Development Committee. Sean also shared a slide show presentation with the committee entitled ***"Learning Scope & Sequence: A Resource for Educators 2018-2020"***, and answered questions from Trustees. Sean expressed thanks to his writing team consisting of Laurie Corrigan - Superintendent of Learning, Alan Morin - St. Catherine CES, Joshua Charpentier - St. Martin CES, Carolyn Farrell - Supervisor of Learning Technologies, Peter Bagnall - Student Achievement Consultant, Lorayne Robertson - Ontario Tech University, Anthony Berardi - Learning Technologies Specialist, and Fr. Paul Massel - Faith Animator.

MOTION: Moved by Helen McCarthy, seconded by Braden Leal that the Policy Development Committee recommend to the Board that new draft Administrative Procedure – ***#322 – Student Digital Privacy*** be received and posted under Directional Policy – ***#300 – Student Achievement and Well-being***.

Carried

2. R.A.: Draft Administrative Procedure – New #505

Performance Appraisal of Employees

Joan Carragher, Superintendent of Learning / Leadership and Human Resource Services, presented new draft Administrative Procedure – ***#505 – Performance Appraisal of Employees*** to the Policy Development Committee and answered questions. Joan will be making minor changes to the Administrative Procedure prior to posting.

MOTION: Moved by David Bernier, seconded by Kevin MacKenzie that the Policy Development Committee recommend to the Board that new draft Administrative Procedure – ***#505 – Performance Appraisal of Employees*** be received and posted under Directional Policy – ***#500 – Employee Relations***.

Carried

3. R.A.: Amendment to Directional Policy
#200 – Catholic Education
Michael Nasello, Director of Education presented revised Directional Policy – ***#200 – Catholic Education*** to the Policy Development Committee and answered questions.

MOTION: Moved by Braden Leal, seconded by Linda Ainsworth that the Policy Development Committee recommend to the Board that revised Directional Policy – ***#200 – Catholic Education,*** be received and posted as amended.

Carried.

4. R.A.: Remove Policies and Administrative Procedures
#203 – Role of Priests in the Schools and
#204 – School Liturgies
Michael Nasello, Director of Education, and Dawn Michie, Superintendent of Learning / I/S Program / Faith and Equity explained to the Policy Development Committee that upon the approval and posting of the ***Pastoral Care in Schools: Diocesan Board Guidelines*** on the Board website, Policies and Administrative Procedures ***#203 – Role of Priests in the Schools*** and ***#204 – School Liturgies*** will be deleted.

MOTION: Moved by David Bernier, seconded by Braden Leal, that the Policy Development Committee recommend to the Board that Board Policies and Administrative Procedures – ***#203 – Role of Priests in the Schools*** and – ***#204 – School Liturgies*** be deleted.

Carried

5. Annual review of Administrative Procedures:
   #508 – Workplace Harassment Prevention
   #509 – Workplace Violence Prevention
   #809 – Occupational Health and Safety
   Joan Carragher, Superintendent of Learning / Leadership and Human Resource Services, presented revised Administrative Procedures – ***#508 – Workplace Harassment Prevention***, ***#509 – Workplace Violence Prevention*** and ***#809 – Occupational Health and Safety*** to the Policy Development Committee and answered questions. Joan will be making minor changes to the Administrative Procedures prior to posting.

MOTION: Moved by Michelle Griepsma, seconded by Braden Leal that the Policy Development Committee recommend to the Board that Administrative Procedures – ***#508 – Workplace Harassment Prevention*** and – ***#509 – Workplace Violence Prevention*** be received and posted under Directional Policy – ***#500 – Employee Relations;*** and that revised Administrative Procedure – ***#809 – Occupational Health and Safety*** be received and posted under Directional Policy ***– #800 – Healthy Schools and Workplaces***.

Carried.

MOTION: Moved by Braden Leal, seconded by David Bernier that the Policy Development Committee Meeting be extended from 8:30 p.m. to 9:00 p.m.

Carried.

C. Information Item:

1. ***Pastoral Care in Schools: Diocesan Board Guidelines***
Michael Nasello, Director of Education and Dawn Michie, Superintendent of Learning / I/S Program / Faith and Equity reviewed the ***Pastoral Care in Schools: Diocesan Board Guidelines*** document and appendices with the Policy Development Committee and answered questions. Michelle Griepsma, Board Chairperson, noted that Trustees do not have a role under Section #3 on page 7, ***ACCOMPANIMENT: Being Partners in Catholic School Communities***. Helen McCarthy stated that she did not support Section #3 quote on page 3 from *Educating Together in Catholic Schools, 2007, p26*. Michael will engage in further conversation with the Bishop regarding the document and will bring it back to the Policy Development Committee.

MOTION: Moved by Michelle Griepsma, seconded by Kevin MacKenzie that the Policy Development Committee receive draft document ***Pastoral Care in Schools: Diocesan Board Guidelines***.

Carried.

D. Next Meeting:

1. Monday, March 30, 2020 6:30 p.m. – 8:30 p.m.

E. Conclusion:

1. Closing Prayer.
The Committee Chairperson, Emmanuel Pinto asked David Bernier to lead the Closing Prayer.

2. Adjournment.

MOTION: Moved by Braden Leal seconded by David Bernier, that the Policy Development Committee Meeting adjourn at 8:50 p.m.

Carried.

Emmanuel Pinto
Committee Chairperson
/ab

Michael Nasello
Director of Education

Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE

Administrative Procedure **Privacy Breach Response**	Administrative Procedure Number **1209**

Directional Policy

Records and Information – 1200

TITLE OF ADMINISTRATIVE PROCEDURE:

Privacy Breach Response

DATE APPROVED:

PROJECTED REVIEW DATE:

May 2025

DIRECTIONAL POLICY ALIGNMENT:

The Privacy Breach Response Administrative Procedure supports Directional Policy 1200 - Records and Information by supporting protection of privacy and the Board's efforts to strategically maintain records and information, adhere to relevant privacy legislation and ensure the efficient creation, maintenance, retrieval, security, storage, and disposition of records.

ALIGNMENT WITH MULTI-YEAR STRATEGIC PLAN:

The Privacy Breach Response Administrative Procedure supports our Vision for achieving Excellence in Catholic Education by supporting the Board's commitment to maintaining a reliable and accessible record of Board actions, transactions and decisions through a coordinated and integrated approach to records and information management.

Strategic Priorities 2017-2020

Vision

Achieving Excellence in Catholic Education
LEARN • LEAD • SERVE

Mission

To educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body and spirit of all.

LEARN

Achieve excellence in instruction and assessment to enable all students to become reflective, self-directed, lifelong learners.

LEAD

Foster critical thinking, creativity, collaboration, and communication, to enable all students to realize their God-given potential.

SERVE

Inspire engagement and commitment to stewardship for creation to enable all students to become caring and responsible citizens.

ACTION REQUIRED:

Peterborough Victoria Northumberland and Clarington (PVNC) Catholic District School Board is committed to the protection of personal and confidential information under its custody or control and to an individual’s right of privacy regarding personal information that is collected, used, retained and disclosed in the school system.

While protection of personal information is paramount, the board recognizes that breaches will occur. This Privacy Breach Response Administrative Procedure allows for a prompt, reasonable and coordinated response when personal information is compromised; that is, when it is collected, accessed, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation.

All employees, members of the Board and third-party providers have a role and responsibility to assist in the containment of a privacy breach.

This administrative procedure outlines the action to be undertaken immediately should a privacy breach or suspected breach occur. It describes the steps necessary to limit the breach and is designed to clarify roles and responsibilities, support effective investigation and containment, and assist with remediation.

PRIVACY BREACH:

a. A privacy breach occurs when personal information is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. PVNC is governed by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Personal Health Information Protection Act (PHIPA). These acts govern the collection, use, disclosure and security of personal information.

b. Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error, such as an individual's personal information being sent by mistake to another individual. In today's environment in which technology increasingly facilitates information exchange, a privacy breach can be more wide-scale.

Examples of potential privacy breaches include:

i. Lost or misplaced personal information, such as a misplaced student assessment, report card or Ontario Student Record (OSR) or a lost USB stick containing student marks or employee contact information.
ii. Stolen technologies or equipment such as laptops, iPads or smart phones that may contain personal information.
iii. Disclosure of personal information to an unauthorized person or group, such as student information forms given to the wrong students or personal information disclosed to a board member, employee or outside agency who did not need it to effectively decide on a matter.
iv. Inappropriate disclosure of personal information, such as two employees discussing and identifying a student in a grocery store, or similar conversation on a cell phone in a public place.
v. Information used for the purpose not consistent with the reason it was collected, such as sharing of staff or contact information for the purpose of sales or marketing or providing personal student information for a third party sponsored contest, without informed consent.

vi. Disposal of equipment with memory capabilities, such as USB sticks, laptops or photocopiers, or paper records containing personal information in a non-secure manner.

vii. Disclosure of personal information via any electronic, message-based or social threat such as ransomware, phishing or extortion.

RESPONSIBILITIES:

All employees and members of the Board are responsible for:

- Being alert to the potential for personal information to be compromised, and therefore potentially playing a role in identifying, notifying, and containing a breach;
- Notifying their supervisor immediately, or, in their absence, the appropriate superintendent or the Freedom of Information (FOI) Officer, upon becoming aware of a breach or suspected breach; and
- Containing, if possible, the suspected breach by suspending the process or activity that caused the breach.

The Board of Trustees is responsible for:

- Ensuring alignment of this administrative procedure with the Records and Information Management Directional Policy;
- Reviewing the Privacy Breach Response Administrative Procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Briefing senior administration and board members as necessary and appropriate;
- Reviewing internal investigation reports and approving required remedial action;
- Monitoring implementation of remedial action; and
- Ensuring that those whose personal information has been compromised are informed as required.

Superintendents, principals, vice-principals, managers and supervisors are responsible for:

- Alerting the FOI Officer of a breach or suspected breach and working with the FOI Officer to implement the five steps of the response protocol;
- Assisting the FOI Officer in obtaining all available information about the nature of the breach or suspected breach, and determining what happened;
- Working with the FOI Officer to undertake all appropriate actions to contain the breach; and
- Ensuring details of the breach and corrective actions are documented.

Freedom of Information (FOI) Officer is responsible for:

- Ensuring that all five steps of the response protocol are implemented;
- Supporting the principal, manager, supervisor and senior administration in responding to the breach; and
- Notifying the Information and Privacy Commissioner where appropriate.

Third-Party Service Providers are responsible for:

- Taking reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements;
- Informing the board contact or FOI Coordinator of all actual and suspected privacy breaches;
- Documenting how the breach was discovered, what corrective actions were taken and reporting back;
- Undertaking a full assessment of the privacy breach in accordance with the third-party service providers' contractual obligations;
- Taking all necessary remedial action to decrease the risk of future breaches; and
- Fulfilling contractual obligations to comply with privacy legislation.

RESPONSE PROTOCOL:

Unauthorized disclosure of personal information is the defining characteristic of a privacy breach, regardless of whether it was intentional, accidental or the result of a theft or malicious intent.

All privacy breaches or suspected privacy breaches must be reported to the principal or supervisor, or in their absence, to the appropriate superintendent or FOI Officer.

Once reported, the supervisor or superintendent will contact the FOI Officer and the following response steps will be implemented.

Step 1 – Respond

- When a suspected privacy breach is identified by an internal or external source, contact the appropriate department to investigate;
- Assess the situation to determine if a breach has indeed occurred and what needs to be done;
- Provide advice on appropriate steps to take to respond to the breach;
- Report the privacy breach to key persons within the Board (including the Director of Education or designate) and, if necessary, to law enforcement;
- Evaluate effectiveness of response to the breach and implement improvement as necessary.

Step 2 – Contain

- Identify the scope of the breach and contain it (e.g., retrieve the hard copies of any personal information that has been disclosed, determine if the breach would allow unauthorized access to any other personal information [e.g., electronic information system], change passwords and identification numbers and/or temporarily shut down the system if necessary to contain the breach);
- Document the breach and containment activities;
- Develop briefing materials;
- Brief the accountable decision maker, senior management, and key persons on the privacy breach and how it is being managed.

Step 3 - Investigate

Once efforts have been made to contain the privacy breach:

- Conduct an investigation with the involvement of other parties as necessary:
  - Identify and analyze the events that led to the privacy breach;
  - Evaluate what was done to contain it; and
  - Recommend remedial action so future breaches do not occur.
- Document the results of internal investigation and use the privacy breach checklist for record keeping, including:
  - Background and scope of the investigation;
  - Legislative implications;
  - How the assessment was conducted;
  - Source and cause of the breach;
  - Inventory of the systems and programs affected by the breach;
  - Determination of the effectiveness of existing security and privacy policies, procedures, and practices;
  - Evaluation of the effectiveness of the response to the breach;
  - Findings including a chronology of events and recommendations of remedial actions;
  - The reported impact of the privacy breach on those individuals whose privacy was compromised.

Step 4 – Notify

- Notify, as required, the individuals whose personal information was disclosed;
- Refer to the below section: “How do you Determine if Notification is Required?”

The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:

- What happened;
- The nature of potential or actual risks or harm;
- What mitigating actions the board is taking;
- Appropriate action to take to protect themselves against harm.

If personal information that could lead to identity theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the Office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's right to complain to the IPC about the Board's handling of their personal information, along with contact information for the IPC.

- Notify appropriate managers and employees within the Board about the breach;
- Report the privacy breach to the Office of the Information and Privacy Commissioner (IPC) as appropriate.

How do you Determine if Notification is Required?

Consider the following factors when determining whether notification is required:

Risk of Physical Harm

Does the loss or theft of information place any individual at risk of physical harm, stalking, or harassment?

Risk of Identity Theft

Is there a risk of identity theft or other fraud as a result of the breach? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).

Risk of Hurt, Humiliation, or Damage to Reputation

Could the loss or theft of information lead to hurt or humiliation or damage to an individual's reputation? This type of harm can occur with the loss or theft of information such as mental health records, medical records, or disciplinary records.

Risk of Loss of Business or Employment Opportunities

Could the loss or theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

Legislative Requirements (PHIPA, Regulation 329/04)

Notice to Affected Individual:

Under the Personal Health Information Protection Act, a Health Information Custodian (HIC), having knowledge that personal health information in their custody or control was lost, stolen or used/disclosed without authority, is required to:

- Notify the individual of the theft or loss or unauthorized use or disclosure of the individual's personal health information; and
- Include in the notice a statement the individual is entitled to make a complaint to the Information Privacy Commissioner.

Notice to the IPC is required when:

- The HIC has reasonable grounds to believe the personal information in their custody or control was used or disclosed without authority by a person who knows or ought to have known they were using or disclosing the information without authority (example: snooping); or
- The HIC has reasonable grounds to believe personal information in their custody or control was stolen (example: stolen records from car, computer hacking); or
- The HIC has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in their custody or control, the personal health information was or will be further used or disclosed without authority (example: a subsequent breach could happen from the initial breach); or
- The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information (example: an automated process results in similar breaches over time); or
- The HIC determines the loss or unauthorized use or disclosure of personal health information is significant taking into consideration the sensitivity and volume of information, the number of individuals affected, and whether more than one HIC was responsible; or
- The HIC is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information (see Notice to College below).

Notice to the IPC generally is not required if:

- The breach was not intentional; and
- The breach was a "one-off" incident and not part of a pattern; and
- The breach is contained; and
- The scope of the breach was not significant; and

- There are no risks of identity theft, physical harm, hurt/humiliation or damage to reputation, or loss of business or employment opportunities.

Notice to College:

A HIC is required to give written notice to their College within 30 days of the following events:

- An individual they have employed as a HIC who is a member of a College, is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal or personal information; or
- The employee resigns and the HIC has reasonable grounds to believe the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

Step 5 - Implement Change

When determining what changes and remedial actions need to be implemented, consider whether it is necessary to:

- Review the relevant information management systems to enhance compliance with privacy legislation;
- Amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information;
- Develop and implement new security or privacy measures, if required;
- Review employee training on legislative requirements, security and privacy policies, procedures, and practices to reduce potential or future breaches, and strengthen as required;
- Test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified;
- Recommend remedial action to the accountable decision maker.

PROGRESS INDICATORS:

- Mandatory annual privacy training for all staff.
- Statistics about breaches involving a theft, loss, or unauthorized use or disclosure of personal information must be submitted to the IPC as part of the Board’s annual statistical report.

DEFINITIONS:

Privacy Breach: A privacy breach occurs when personal information is stolen or lost or is collected, used or disclosed without authority.

Personal information: Information about an identifiable or potentially identifiable individual, as defined under privacy legislation.

Third-party Service Providers: Contracted third parties used to carry out or manage programs and/or services on behalf of the board. For the purpose of privacy breach reporting, third party includes all contractors that receive personal information from the board or collect personal information on behalf of the board.

SUPPORTING DOCUMENTS:

- Appendix A: Sample Privacy Breach Report
- 1202 - Protection of Privacy AP
- 1207 – Freedom of Information AP
- Personal Information Management Training Video

REFERENCES:

- *Education Act*
- *Municipal Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Protection Act*

APPENDIX A

Sample Privacy Breach Report

BREACH REPORT # ______________

Take immediate action when you have been advised of a suspected privacy breach. Many of the steps outlined below have to be carried out simultaneously or in quick succession. Steps 1 and 2 are completed based on the information received either directly from an employee, or verbally through their immediate supervisor (e.g., phone call), or in written form (e.g., email).

STEP 1 – Respond, and STEP 2 – Contain

1. Person Reporting Suspected Breach:

First name: ________________________ Last name: ____________________________

Job title: __________________________ Location (school/department): _____________

Name of immediate supervisor: ___________________________________

Phone number: ____________________________

2. When Incident Occurred: Date: ____________________ Time: __________________

(mm/dd/yyyy) (Indicate A.M. or P.M.)

3. Incident Details:

Number of individuals whose information was accessed without consent or authorization:

Type of personal information that was accessed without consent or authorization, e.g., health/medical information, student marks, biographical information (such as home address, phone numbers, names and contact information of family members), behaviour concerns, etc.

Whom the personal information belongs to and **how many individuals were affected** (e.g., student, employee, third party [someone who is neither a student nor employee of the board, such as a parent/ guardian or volunteer]):

Who had unauthorized access to the personal information, and **how** that access was made:

Efforts made, if any, to contain the privacy breach (e.g., suspending the process/activity that caused the breach)

STEP 3 – Investigate

Following a report of a suspected privacy breach, ensure that the activity/process has been contained if possible. Conduct an investigation of the information supplied in Steps 1 and 2 of this report in conjunction with current privacy legislation (MFIPPA, PHIPA, PIPEDA) and with local privacy policies and procedures to determine if the incident is, in fact, a breach. Note: You may wish to consult legal counsel to assist you in your investigation.

If a breach HAS NOT occurred:

Contact the person who reported the suspected breach **and** their immediate supervisor to advise them of your determination. No further action is required by the employee or supervisor.

STEP 4 – Notify

If a breach HAS occurred, notify the following individuals as appropriate:

- □ Individuals whose privacy was breached
- □ Senior administration/managers/principals
- □ IPC*
- □ Accountable decision maker (Director of Education)
- □ Legal counsel
- □ Other:________________________________

* Note: The type and extent of the breach will influence your decision to notify the Information and Privacy Commissioner's Office, Toronto (1-800-387-0073) 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8.

STEP 5 – Implement Change

Steps taken to correct the problem:

- □ Develop, change, or enhance policies and procedures
- □ Ensure strengthening of security and privacy controls
- □ Advise IPC of investigation findings and corrective action
- □ Other:

Provide additional notices (as deemed appropriate):

□ Relevant third parties
□ Consider public announcement (e.g., statement and/or apology)
□ Other Ontario school boards/authorities (where shared responsibilities exist)

Prevent future breaches:

□ Arrange employee training on privacy and security
□ Recommend appropriate and necessary security safeguards
□ Consider having an outside party review processes and make recommendations (e.g., auditing company)
□ Evaluate the effectiveness of remedial actions

The Privacy Officer/FOI Coordinator may wish to review school board/authority policies, procedures, practices, and training materials to ascertain whether any revisions are required to ensure a clearer understanding of what constitutes a privacy breach.

Sign-off

The Director of Education or designate (e.g., Privacy Officer/FOI Coordinator) is required to sign below to formally acknowledge that the breach was handled in accordance with privacy legislation and with the school board's/authority's policies and procedures:

______________________________	______________________________
Print Name/Title	Signature

Sign-Off Date: ____________________
(mm/dd/yyyy)

Resources

AICA/CICA Privacy Taskforce, *Incident Response Plan 2003*
(American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants)

Government of Ontario, Ontario Shared Services, *Privacy Review 2005*

Information and Privacy Commissioner/Ontario, *Breach Notification Assessment Tool, December 2006*

Information and Privacy Commissioner/Ontario, *What to do if a Privacy Breach Occurs: Guidelines for Government Organizations*, May 2003

The Office of the Chief Information and Privacy Officer, Taking the Right Steps - *A Guide to Managing Privacy and Privacy Breaches*, revised April 18, 2007

Information and Privacy Commissioner, *Online Educational Services, What Educators Need to Know, November 2016*

https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/

B.1.

Recommended Action:

That the Policy Development Committee recommend to the Board that new draft Administrative Procedure –

#1209 – Privacy Breach Response

be received and posted under Directional Policy –

#1200 – Records and Information.

Carried

Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure **Personal Network Devices**	*Administrative Procedure Number* **314** **(NEW)** **904** **(OLD)**
Directional Policy **300: Student Achievement and Well Being**	

TITLE OF ADMINISTRATIVE PROCEDURE:

Personal Network Devices

DATE APPROVED: March 30, 2020

PROJECTED REVIEW DATE:

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 Network 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.

Strategic Priorities 2017-2020

Vision

Achieving Excellence in Catholic Education
LEARN • LEAD • SERVE

Mission

To educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body and spirit of all.

LEARN

Achieve excellence in instruction and assessment to enable all students to become reflective, self-directed, lifelong learners.

LEAD

Foster critical thinking, creativity, collaboration, and communication, to enable all students to realize their God-given potential.

SERVE

Inspire engagement and commitment to stewardship for creation to enable all students to become caring and responsible citizens.

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 Network 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 student, access and/or monitor the Board’s Electronic Information Systems. Principals will be informed of any serious infraction of the Student Acceptable Use of Technology Policy. Disciplinary actions of a student 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 Network 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

Manager of Information Technology is responsible for:

- Monitoring usage of the board's network systems.
- Ensuring the use of Personal Network Devices does not impact the integrity of the Board's technology systems.
- Determining, at the Board's discretion, the access provided for Personal Network Devices:
  - The type of access (wired, wireless, no access)
  - Suitability of any device to be connected
  - Resources available when connected (internet only, local web, and/or server access).
- Monitoring the use of Personal Network 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.

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

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
    - 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.

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 Network Device to store "personal information" as defined in the Municipal Freedom of Information and Protection of Privacy Act.

Students are responsible for:

- Using available technology to further their educational goals and promote Catholic teaching and at the discretion of an Educator.
- Reading and acknowledging 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 is:
  - for educational purposes, as directed by an educator
  - for health and medical purposes
  - to support special education needs

All users of Personal Network Devices are responsible for:

- Ensuring their Personal Network 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 they do not connect a Personal Network Device to the Board's network which allows network access over and above what is provisioned by the Board. These Devices include, but are not limited to, modems, routers, wireless access points and cellular hotspots.

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.

PROGRESS INDICATORS:

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

DEFINITIONS:

- **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.
- **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.
- **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 Network Device** – A device, owned by the user, which has the capability to connect to a computer network, either through a network wire or using a radio designed to connect to a wireless computer network. Examples include: laptops, netbooks, some portable music players, some portable game devices and some cellular telephones.
- **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

B.2.

Recommended Action:

That the Policy Development Committee recommend to the Board that Policy and Administrative Procedure – ***#904 – Personal Network Devices***, be deleted and the revised, newly formatted, Administrative Procedure – ***#314 – Personal Network Devices***, be received and posted as amended under Directional Policy – ***#300 – Student Achievement and Well-being***.

Carried

B.3.

Recommended Action:

That the Policy Development Committee recommend to the Board that Policies and Administrative Procedure –

#602 – (Old Policy #105)

School Sites – Operating Budget Surplus

#603 – (Old Policy and Administrative Procedure #106)

Alternative Arrangements for School Facilities

be deleted.

Carried

Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
ADMINISTRATIVE PROCEDURE **VISITORS TO SCHOOLS**	*ADMINISTRATIVE PROCEDURE NUMBER* **902 (NEW)** **411 (OLD)**
Directional Policy **900 – Safe and Accepting Schools**	

DRAFT

TITLE OF ADMINISTRATIVE PROCEDURE:
Visitors to Schools

DATE APPROVED:
X

PROJECTED REVIEW DATE:
x

DIRECTIONAL POLICY ALIGNMENT:
This Administrative Procedure aligns with the Safe and Accepting Schools Directional Policy - 900 by ensuring our schools are welcoming, safe, respectful, equitable, inclusive and accepting learning and teaching environments, rooted in the teachings of the Gospel.

ALIGNMENT WITH MULTI-YEAR STRATEGIC PLAN:
The Visitors to Schools Administrative Procedure supports our Mission to educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body, and spirit of all.

The Board is committed to providing a welcoming school environment for visitors and a safe learning environment for all students and staff.

Strategic Priorities 2017-2020

Vision
Achieving Excellence in Catholic Education
LEARN • LEAD • SERVE

Mission
To educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body and spirit of all.

LEARN
Achieve excellence in instruction and assessment to enable all students to become reflective, self-directed, lifelong learners.

LEAD
Foster critical thinking, creativity, collaboration, and communication, to enable all students to realize their God-given potential.

SERVE
Inspire engagement and commitment to stewardship for creation to enable all students to become caring and responsible citizens.

ACTION REQUIRED:
The Peterborough Victoria Northumberland and Clarington Catholic District School Board’s Visitors to Schools Administrative Procedure provides direction to administrators to develop processes for managing visitors to schools for the protection of our students and staff. These procedures apply to all visitors while on school property.

To facilitate a welcoming and safe environment, each school will:

- have signage that directs all visitors to start their visit at the school main office;
- have a Visitor’s Book available in the main office for all visitors to sign in and out. The Visitor’s Book will indicate the date, time, and purpose of each visit; and
- have a form of identification (badge, button) that will identify each visitor to the building and grounds. The identification badge/button will designate the role of each visitor. The badge/button shall be worn and visible to the school community for the duration of the visit.

RESPONSIBILITIES:

The Board of Trustees is responsible for:

- ensuring alignment with the Safe and Accepting Schools Directional Policy; and
- reviewing the Visitors to Schools Administrative Procedure as part of its regular policy and procedures review cycle.

The Director of Education is responsible for:

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

Superintendent of Safe Schools is responsible for:

- reviewing and revising this administrative procedure as necessary.

Superintendent of Schools are responsible for:

- supporting principals in the implementation of this administrative procedure.

Principals are responsible for:

- ensuring that all visitors are familiar with safety procedures specific to the building and grounds;
- maintaining a visitor’s book in the school and ensuring that all visitors sign in and out of the building;
- ensuring that all visitors wear a badge/button and that it is visible to the school community for the duration of the visit;
- ensuring that all visitors are screened for appropriate access to staff and students. This may include referring to Maplewood or the Ontario Student Record (OSR) for special custody notes;
- ensuring all visitors to schools procedures are widely circulated and publicized within the school, and in the school community, during the first week of school; and
- refusing to admit to the school, a person whose presence in the school would, in the principal’s judgement, be detrimental to anyone in the school.

Teachers and Staff are responsible for:

- supporting the implementation of this Administrative Procedure;
- redirecting to the main office, an individual in the school that is found to be on the property without proper identification; and
- informing the principal if they have knowledge of any person not being suitable as a visitor.

Visitors are responsible for:

- reporting to the main office immediately upon arrival;
- sharing the purpose and location of their visit with the principal or his or her designate;
- signing in and out of the Visitor’s Book
- wearing the badge/button provided for the duration of the visit;
- respecting and following the school’s procedures; and
- being respectful and demonstrating appropriate conduct while on Board property.

PROGRESS INDICATORS:

- Schools develop and implement processes for managing visitors to schools;
- Visitors to Schools Program procedures are communicated throughout the school community;
- Schools provide a welcoming school environment for visitors; and
- Schools provide a safe learning environment for all students and staff.

DEFINITIONS:

Visitor - a visitor can be:

a) a parent, guardian, or family member of a child attending a Roman Catholic school;
b) a member of the board that operates the school;
c) a member of the Legislature in the member's constituency, with prior approval of the board
d) a member of the clergy of the Roman Catholic Church in the area where the member has pastoral charge; or
e) any other person who is not on the current staff register for the school.

REFERENCES:

Education Act

Part II.1, Section 50 (1-3)
Part X, Section 265 (M-N)
Ontario Regulation 298

Municipal Freedom of Information and Protection of Privacy Act
AP 601, Community Use of Board Facilities
AP 403, Emergency Management and Business Continuity Program
AP 707, Volunteers in Our Schools
AP 909, Code of Conduct

B.4.

Recommended Action:

That the Policy Development Committee recommend to the Board that Policy and Administrative Procedure – ***#411 – Visitors to Schools***, be deleted and the revised, newly formatted, Administrative Procedure – ***#902 – Visitors to Schools***, be received and posted as amended under Directional Policy – ***#900 – Safe and Accepting Schools***.

Carried

Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE

ADMINISTRATIVE PROCEDURE	*ADMINISTRATIVE PROCEDURE NUMBER*
SAFE ARRIVALS	**901 (NEW)** **814 (OLD)**

Directional Policy

900 – Safe and Accepting Schools

DRAFT

TITLE OF ADMINISTRATIVE PROCEDURE:

Safe Arrivals

DATE APPROVED:

X

PROJECTED REVIEW DATE:

x

DIRECTIONAL POLICY ALIGNMENT:

This Administrative Procedure aligns with the Safe and Accepting Schools Directional Policy - 900 by ensuring our schools are welcoming, safe, respectful, equitable, inclusive and accepting learning and teaching environments, rooted in the teachings of the Gospel.

ALIGNMENT WITH MULTI-YEAR STRATEGIC PLAN:

The Safe Arrivals Administrative Procedure supports our Mission to educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body, and spirit of all.

The Board recognizes that it is a shared responsibility of parent(s)/guardian(s), school administration, and school staff to ensure the safety of students.

Strategic Priorities 2017-2020

Vision

Achieving Excellence in Catholic Education
LEARN • LEAD • SERVE

Mission

To educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body and spirit of all.

LEARN
Achieve excellence in instruction and assessment to enable all students to become reflective, self-directed, lifelong learners.

LEAD
Foster critical thinking, creativity, collaboration, and communication, to enable all students to realize their God-given potential.

SERVE
Inspire engagement and commitment to stewardship for creation to enable all students to become caring and responsible citizens.

ACTION REQUIRED:
The Peterborough Victoria Northumberland and Clarington Catholic District School Board’s Safe Arrivals Administrative Procedure provides direction to school administrators to develop a school-based Safe Arrival Program.

Safe Arrival Programs are a mechanism that parent(s)/guardian(s) and school staff will use to account for any student’s unexplained failure to arrive at school. The Safe Arrivals Program is a collaborative responsibility.

Parent(s)/guardian(s) are responsible for communicating planned student absences or lateness to the school on a timely basis. This information will be reconciled with information obtained through classroom attendance-taking procedures. Parent(s)/guardian(s) are responsible for providing the school with complete and current emergency information to enable the school to make any necessary follow-up communication.

The Safe Arrival Program will include:

- a reliable method for parent(s)/guardian(s) to communicate planned student absences or lateness to the school on a timely basis;
- a process to parent(s)/guardian(s) for updating emergency contact information;
- daily school attendance-taking procedures;
- the steps that are to be taken when a student fails to arrive at school;
- consideration for both normal and recurring circumstances, as well as unusual events and conditions. *For example, regular procedures could be modified on days when students are likely to arrive late because of inclement weather or bus cancellations*;
- a plan for training for individuals involved in supporting the Safe Arrival Program;
- periodic review for effectiveness.

RESPONSIBILITIES:

The Board of Trustees is responsible for:

- ensuring alignment with the Safe and Accepting Schools Directional Policy; and
- reviewing the Safe Arrivals Administrative Procedure as part of its regular policy and procedures review cycle.

The Director of Education is responsible for:

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

Superintendent of Safe Schools is responsible for:

- reviewing and revising this administrative procedure as necessary.

Superintendents of Schools are responsible for:

- supporting principals in the implementation of this administrative procedure.

Principals are responsible for:

- consulting with school staff, parent(s)/guardian(s), and Catholic School Council to develop the Safe Arrival Program;
- implementing and maintaining the Safe Arrival Program;
- communicating the procedures and the roles and responsibilities to school staff and parent(s)/guardian(s);
- conducting training for individuals involved in supporting the Safe Arrival Program;
- ensuring that occasional staff are familiar with the school’s Safe Arrival procedures;
- communicating Safe Arrival Program procedures throughout the school community at the beginning of the school year, and with new registrants as part of the intake process;
- ensuring daily attendance procedures are completed to support the Safe Arrival Program;
- ensuring timely communication is made with parent(s)/guardian(s) in the event of a student’s unexplained failure to arrive at school;
- notifying the police if there are concerns regarding a student’s absence; and
- notifying the Family of School’s Superintendent if and when police have been contacted.

Secretaries are responsible for:

- supporting the implementation of this Administrative Procedure;
- reconciling parent(s)/guardian(s) reported student absences or lateness information received with information received through classroom attendance-taking procedures; and
- enacting the procedures for communicating with parent(s)/guardian(s) in the event of a student’s unexplained failure to arrive at school.

Teachers are responsible for:

- supporting the implementation of this Administrative Procedure;
- recording accurate daily attendance; and
- submitting the daily attendance in a timely manner to support the school's Safe Arrival Program Procedures.

Parent(s)/Guardian(s) are responsible for:

- their children's safety until they arrive at school, are picked up by school transportation, and/or they have left the school, or are dropped off by the school transportation;
- communicating planned student absences or lateness to the school on a timely basis; and
- providing the school with complete and current emergency contact information.

PROGRESS INDICATORS:

- Schools develop and implement Safe Arrival Programs; and
- Safe Arrival Program procedures are communicated throughout the school community.

DEFINITIONS:

Inclement Weather - refers to severe weather conditions, including ice, fog, sleet, snow, flood, extreme temperatures, and/or wind, which are considered serious enough to raise concerns regarding the safety of students and staff.

REFERENCES:

Ministry of Education Policy/Program Memorandum #123, "Safe Arrivals", dated February 2, 1999
AP 909, Code of Conduct
AP 902, Visitors to Schools

B.5.

Recommended Action:

That the Policy Development Committee recommend to the Board that Policy and Administrative Procedure – ***#814 – Safe Arrivals – Elementary***, be deleted and the revised, newly formatted, Administrative Procedure – ***#901 – Safe Arrivals***, be received and posted as amended under Directional Policy – ***#900 – Safe and Accepting Schools***.

Carried