

Policy Development Committee Meeting

Tuesday, November 1, 2022

6:30 – 8:30 p.m.

Catholic Education Centre – Large Boardroom

Chairperson: Kevin MacKenzie

Trustees who are unable to attend are asked to please notify
Michelle Kennedy Administrative Assistant at
mkennedy@pvnccdsb.on.ca

A. Call to Order:

1. Opening Prayer.
Jenny Leahy
2. Land Acknowledgement.
3. Approval of the Agenda.
4. Declarations of Conflicts of Interest.
5. Approval of the minutes of the Policy Development Committee, October 4, 2022. Page 3
6. Business Arising from the Minutes.

B. Presentations / Recommended Actions:

1. R.A.: Revised Administrative Procedure – AP #1106, Display of Flags. Page 8
Galen Eagle, Manager of Communications.
2. R.A.: New Administrative Procedure – AP #602, Cybersecurity Page 14
Sean Heuchert, Manager of Information Technology.
3. R.A.: Revised Administrative Procedure – AP #803, Pediculosis in Schools. Page 35
Jonathan Di Ianni, Superintendent of Learning.
4. R.A.: Revised Administrative Procedure – AP #1302, Bus Operator Contracted Services. Page 49
Isabel Grace, Superintendent of Business, Finance and Facilities Services.

5. R.A.: Revised Administrative Procedure – AP #1305, Accidents Involving School Purpose Vehicles.

Page 58

Isabel Grace, Superintendent of Business, Finance and Facilities Services.

C. Information Items:

D. Next Meeting:

1. Tuesday, February 7, 2022, 6:30 p.m.

E. Conclusion:

1. Closing Prayer
Linda Ainsworth.
2. Adjournment.

Minutes

The Minutes of the Policy Development Committee Meeting held on Tuesday, October 4, 2022, at 6:30 p.m., in person at the Catholic Education Centre and virtually by Google Meet.

Present:

Trustees: Linda Ainsworth, Loretta Durst, Jenny Leahy, Braden Leal, Kevin MacKenzie (Committee Chairperson), Madelyn Gaskell (Student Trustee).

Administration: Jeannie Armstrong, Joan Carragher, Galen Eagle, Sean Heuchert.

Recorder: Michelle Kennedy.

Regrets: Siobhan Marie (Student Trustee) and Helen McCarthy.

A. Call to Order:

1. Opening Prayer.

Kevin MacKenzie, Committee Chairperson, called the meeting to order at 6:30 and invited Trustee Braden Leal to lead the committee in opening prayer.

2. Land Acknowledgement.

Kevin MacKenzie respectfully acknowledged that the Policy Development Committee Meeting was taking place on the treaty and traditional territory of the Mississauga Anishinaabeg.

Following the Land Acknowledgment, the chairperson noted that October 4th was World Teachers' Day. He expressed his thanks and appreciation for all teachers in our board and their daily impact on our students.

3. Approval of the Agenda.

MOTION: Moved by Braden Leal, seconded by Jenny Leahy
that the agenda be approved.

Carried.

4. Declarations of Conflicts of Interest.

There were no conflicts of interest declared.

5. Approval of the Minutes of the Policy Development Committee Meeting, May 17, 2022.

MOTION: Moved by Linda Ainsworth, seconded by Loretta Durst

that the minutes of the Policy Development Committee Meeting held on Tuesday, May 17, 2022, be approved.

Carried.

6. Business Arising from the Minutes.

There was no business arising out of the minutes.

B. Presentations/Recommended Actions:

1. New Administrative Procedure – AP #512, Electronic Monitoring.

Sean Heuchert reviewed the key points of the new administrative procedure with a slide show presentation. New provincial legislation requires the board to put this administrative procedure in effect.

MOTION: Moved by Loretta Durst, seconded by Jenny Leahy

that the Policy Development Committee recommend to the Board that Administrative Procedure #512, Electronic Monitoring, be received and posted under Directional Policy #500, Employee Relations.

Carried.

2. Revised Administrative Procedure – AP #1204, Custody Access to Students.

Galen Eagle, Manager of Communications, reviewed the scope of applicable legislation relating to Administrative Procedure #1204 and highlighted the proposed revisions. Questions from the trustees were answered and suggested changes were noted.

MOTION: Moved by Braden Leal, seconded by Jenny Leahy

that the Policy Development Committee recommend to the Board that Administrative Procedure #1204, Custody Access to Students, be

received and posted as amended under Directional Policy #1200, Records and Information.

Carried.

3. Revised Administrative Procedure – AP #1205, Copyright Protected Acts.

Galen Eagle, Manager of Communications gave a presentation to review Administrative Procedure #1205 that is scheduled for renewal. A demonstration of the online tool that is used by educators to determine possible copyright infringement on a resource was given by Galen Eagle.

MOTION: Moved by Braden Leal, seconded by Loretta Durst
that the Policy Development Committee recommend to the Board that Administrative Procedure #1205, Copyright Protected Acts, be received and posted as amended under Directional Policy #1200, Records and Information.

Carried.

4. Remove Board Policy and Administrative Procedure –#309, Historical Archives.

Galen Eagle, Manager of communications gave background information and rationale for the proposal to delete Board Policy and Administrative Procedure #309, Historical Archives, citing that relevant content was incorporated into Administrative Procedure #1201 when it was last revised.

MOTION: Moved by Jenny Leahy, seconded by Loretta Durst
that the Policy Development Committee recommend to the Board that Board Policy #309, Historical Archives, and the corresponding Administrative Procedure and Appendices be deleted.

Carried.

5. New Administrative Procedure – AP #201, School/Parish Accompaniment.

Jeannie Armstrong, Superintendent of Special Education, Faith and Equity, explained the history and evolution of the new administrative procedure which encompasses process and direction from an older policy and administrative procedure.

MOTION: Moved by Linda Ainsworth, seconded by Loretta Durst

that the Policy Development Committee recommend to the Board that Administrative Procedure #201, School/Parish Accompaniment, be received and posted under Directional Policy #200, Catholic Education; and,
that Board Policy #812, Role of the Priest in the School, and the corresponding Administrative Procedure, be deleted.

Carried.

6. New Administrative Procedure – AP #202, Board Diocesan Relations.

Jeannie Armstrong, Superintendent of Special Education, Faith and Equity, reviewed the components of the new administrative procedure and explained the background of the documents and the integration of Board Policy and Administrative Procedure #811, School Liturgies into the proposed administrative procedure. Jeannie Armstrong addressed questions from the trustees.

MOTION: Moved by Linda Ainsworth, seconded by Braden Leal

that the Policy Development Committee recommend to the Board that Administrative Procedure #202, School Liturgies, be received and posted as amended under Directional Policy #200, Catholic Education; and,
that Board Policy #811, School Liturgies, and the corresponding Administrative Procedure, be deleted.

Carried.

C. Information Items:

1. St. Paul Catholic Elementary School, Norwood, 50th Anniversary. Saturday, November 5th, 2022. Doors open at 2 pm, Mass at 5 pm.

D. Next Meeting:

1. Tuesday, November 1, 2022, 6:30 p.m.

E. Conclusion:

1. Closing Prayer:

The Committee Chairperson asked Loretta Durst to lead the prayer to close the meeting.

2. Adjournment:

MOTION: Moved by Braden Leal, seconded by Jenny Leahy
that the meeting be adjourned at 7:44 p.m.

Carried.

Draft

Recommended Action:

that the Policy Development Committee recommend to the Board that Administrative Procedure #1106, Display of Flags, be received and posted as amended under Directional Policy #1100, Communications; and

that Board Policy #1108, Display of Flags, and the corresponding Administrative Procedure #1108, be deleted.



BOARD ADMINISTRATIVE PROCEDURE	
<i>Administrative Procedure</i> Display of Flags	<i>Administrative Procedure Number</i> 1106
<i>Directional Policy</i> 1100 Communications	

Title of Administrative Procedure:

Display of Flags

Date Approved:

November, 2022

Projected Review Date:

2027

Directional Policy Alignment:

The Display of Flags Administrative Procedure aligns with Directional Policy 1100 – Communications by setting appropriate protocols for displaying the National Flag of Canada and other flags on Peterborough Victoria Northumberland and Clarington Catholic District School Board properties.

Alignment with Multi-Year Strategic Plan:

The Display of Flags Administrative Procedure supports the Board's Multi-Year Strategic Plan to inspire faith, ensure equity, value relationships, and maximize resources.

[PVNCCDSB Board Vision, Mission and Strategic Priorities](#)

Action Required:

- 1) The National Flag of Canada shall be flown at the Catholic Education Centre, all schools, and all Board facilities.
- 2) Each Board facility shall display inside the school or Board facility the National Flag of Canada, the Provincial Flag of Ontario, and the Vatican (Papal) Flag. The Vatican (Papal) Flag should always be displayed horizontally.
- 3) The Director of Education may approve and direct the display of other flags as deemed appropriate to further the Board's mission, vision and strategic priorities outlined in the Board's Multi-Year Strategic Plan.
 - a) All schools and Board facilities shall fly the Pride Flag from June 1 to June 30 in recognition of Pride Month to further the promotion of an environment of inclusion, diversity and equity in our community.
- 4) Where there are multiple flags displayed together, the National Flag of Canada shall be displayed above any other flag and should always receive precedence.
- 5) As Canada's paramount symbol of national identity, the act of flying the National Flag of Canada at half-mast is a dramatic visual statement that speaks to the shared sense of collective loss. Flags at Peterborough Victoria Northumberland and Clarington Catholic District School Board schools and facilities shall be flown at half-mast upon the direction of the Director of Education or designate.
 - a) Flags are flown at half-mast in recognition of the death of prominent public figures and other individuals.
 - b) On Remembrance Day, flags at all schools and Board facilities shall be flown at half-mast from 11 a.m. to the end of the instructional day.
 - c) On National Truth and Reconciliation Day, flags at all schools and Board facilities shall be flown at half-mast from sunrise to sunset.
- 6) Individual schools, at the direction of the principal and in consultation with their supervisory officer, may fly their flag at half-mast to recognize the death of a student or staff member or an individual whose death has a significant impact on the school community.

- 7) Proper etiquette should be maintained when displaying flags on board property, and staff, students and visitors must always treat all flags with dignity and respect. (See resource section for rules for flying and displaying the National Flag of Canada).
- 8) Flags should be regularly inspected for signs of wear and damage and shall be replaced when worn, noticeably faded or otherwise unfit for service. When a flag is worn and is no longer in a suitable condition for use, it should be destroyed in a dignified way.
- 9) When raised or lowered, a flag should be prevented from touching or falling to the ground.
- 10) Flags should never be used as a table or seat cover; be used as a barrier; drape the front of a dais or podium; or be allowed to touch the floor or ground under any circumstances.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment of this administrative procedure with the Communications Directional Policy.
- Reviewing this 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 of and compliance with this Administrative Procedure.
- Approving and directing the display of other flags on Board property as deemed appropriate to further the Board's mission, vision and strategic priorities outlined in the Board's Multi-Year Strategic Plan.
- Directing the flying of Board flags at half-mast as appropriate or designating this duty to an appropriate staff person.

Superintendents of Schools and System Portfolios are responsible for:

- Ensuring school principals are consistent with the application of this Administrative Procedure.

- Ensuring that any employee for whom they have supervisory responsibility are aware of the requirements under this Administrative Procedure.
- Assist the school principal with responsibilities and duties as assigned.

Principals are responsible for:

- Ensuring the lowering of flags to half-mast is performed on school property as directed by the Director or designate.
- Informing their supervisory officer and Communication Services of a local circumstance that may necessitate the lowering of the school's flag to half-mast.
- Maintaining proper etiquette when displaying flags on school property, and ensuring staff, students and visitors treat all flags with dignity and respect.

Staff are responsible for:

- Treating all flags with dignity and respect.
- Familiarizing themselves with flag etiquette and protocol when arranging flag displays at school.

Students are responsible for:

- Treating all flags with dignity and respect.
- Familiarizing themselves with flag etiquette and protocol when arranging flag displays at school.

Communication Services is responsible for:

- Communicating and providing appropriate context to the public when flags are to be flown at half-mast.

Progress Indicators:

- The effectiveness of the policy will be evaluated on an as needed basis.

Resources:

[Rules for flying the National Flag of Canada](#)

[Rules for half-masting the National Flag of Canada](#)

Definitions:

Half-Mast: the position of the flag when flying at half-mast will depend on its size, the length of the mast and its location; but, as a general rule, the centre of the flag should be exactly half-way down the mast. When hoisted to or lowered from half-mast position, a flag should be first raised to the masthead.

Draft

Recommended Action:

That the Policy Development Committee recommend to the Board that Administrative Procedure #602, Cybersecurity, be received and posted under Directional Policy #600, Stewardship of Resources.



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

Title of Administrative Procedure:

Cybersecurity

Date Approved:

TBD

Projected Review Date:

October 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](#)



*Peterborough Victoria
Northumberland and Clarington
Catholic District School Board*

CYBERSECURITY HANDBOOK

Table of Contents

Principles	3
1. Cybersecurity Governance	4
2. Compliance with Legal and Ministry Requirements	4
3. Security of Sensitive Information	4
4. Cyber Risk Management	5
5. Supply Chain, Cloud and Third-Party Service Providers	6
6. Availability and Reliability of Technology	6
7. Network and Endpoint Security	7
8. Incident and Breach Response Planning and Management	7
9. Monitoring and Logging	8
10. Vulnerability and Patch Management	8
11. Access Control and Authorization	9
12. Privacy and Data Protection	10
13. Cyber Awareness Training	10
14. Exceptions	11
15. Contact	11
Appendix A - Glossary	12
Appendix B - References	16

Principles

- 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.
- Cybersecurity shall be provided in a manner that serves the security and safety of students and staff while adhering to legislative requirements.
- 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.
- 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.
- The school 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.
- The Board aims to facilitate secure, safe, responsible and respectful use of technology as is further defined in the board's acceptable use of technology 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.

This document uses the following wording conventions:

Shall – The requirement is mandatory. Without it, the organization is not considered protected and deemed to be at a greater risk of cyber threats. If a mandatory requirement is currently not met, the board shall have a documented plan for remediating identified gaps.

Should – The requirement ought to be adhered to, unless there is a documented and approved business rationale for not adhering to it.

1. Cybersecurity Governance

- 1.1. A comprehensive board-wide Administrative Procedure on Cybersecurity shall be developed, implemented, communicated and maintained up to date.
- 1.2. The accompanying “Handbook” (this document) will be updated and reviewed with IT Services staff annually and with other stakeholders as part of the regular Administrative Procedure review process.
- 1.3. Comprehensive board standards, procedures and guidelines for cyber security, cyber safety and the protection of online privacy shall be developed, implemented, communicated and maintained up to date in accordance with the direction and priorities established by the board’s governance.
- 1.4. The board shall establish and maintain Cybersecurity as an integral part of the multi-year technology plan.
- 1.5. Authorized users shall comply with the Cybersecurity administrative procedure and the board’s Cybersecurity standards, procedures and guidelines, as applicable.
- 1.6. The board shall develop and maintain a catalog of board allowed applications and board staff shall only use applications identified in this catalog. Staff shall have the ability to request additions and changes to this catalog. All applications shall be subject to an application vetting process to assess privacy and data security risks, to determine inclusion or exclusion from the catalog.

2. Compliance with Legal and Ministry Requirements

- 2.1. The board’s Cybersecurity measures shall comply with all applicable laws, legislations and Ministry of Education policy directives.

3. Security of Sensitive Information

- 3.1. The board shall ensure individuals undergo personnel security screening commensurate to the duties they perform prior to being granted access to board sensitive information, information systems, and any board owned and managed IT or network-connected IT resources.
- 3.2. The board shall ensure authorized users of board IT and network connected OT resources:
 - 3.2.1. Are aware of their Cybersecurity responsibilities;

- 3.2.2. Adhere to the board's Cybersecurity standards, procedures and guidelines as applicable to their role(s); and
- 3.2.3. Receive cyber protection awareness training to the extent necessary by their role(s) and level of access.

4. Cyber Risk Management

- 4.1. With increased reliance on technology, digital processes and the internet, the board recognizes that cyber risks have the potential to affect all aspects of the board, its staff and students, and reputation.
- 4.2. The board recognizes cyber risk management as an important practice that enables the board to align cyber security, cyber safety and digital privacy with board business objectives and business risk, ensuring the most effective and efficient way to mitigate against cyber risks.
- 4.3. As an integral part of cyber risk management, the board shall classify IT and network-connected OT assets to determine the level of information sensitivity and risk to the assets, and appropriate levels of safeguards needed to protect them. The classification level shall be determined by assessing the requirement for confidentiality of information, integrity and availability of information and systems.
- 4.4. Any new IT solution and network-connected OT solution in the board shall undergo an assessment of cyber risks prior to entering into a contract or service agreement, and prior to implementation. For cloud services, the assessment may be of evidence in the form of an attestation providing reasonable assurance regarding the presence and correct operation of safeguards within a service.
- 4.5. The board shall do a re-assessment of cyber risks if there are any significant changes to a board's IT solution, network-connected OT solution and/or the K-12 threat environment, and when deemed necessary.
- 4.6. All identified risks shall have a designation of who is responsible for their treatment, management and oversight with the Director of Education being ultimately accountable for all cyber risks in the board. Depending on the nature of the identified risk, responsibility for its risk treatment plan and its implementation may reside with the business owner, service owner, service provider or vendor.
- 4.7. The board shall monitor risk compliance for IT and network-connected OT resources deemed critical to the board. This may be done in the form of cyber risk assessments, penetration tests, vulnerability assessments, privacy impact assessments and other industry established practices.
 - 4.7.1. Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

5. Supply Chain, Cloud and Third-Party Service Providers

- 5.1. The board recognizes that cyber risks associated with a vendor's supply chain, third-party service providers, contractors, and cloud providers are important areas requiring coordinated risk mitigation efforts. Areas of third-party cyber risk include:
 - 5.1.1. Access by third-party service providers or vendors - virtual or physical access to board technology, IT system and sensitive information.
 - 5.1.2. Suppliers with poor cyber security and privacy protection practices.
 - 5.1.3. Software, hardware and cloud services with vulnerabilities, compromised systems or embedded malware.
 - 5.1.4. Cyber security vulnerabilities in supply chain management or supplier systems.
 - 5.1.5. Third-party data storage or data aggregators.
 - 5.1.6. Contract terms and conditions, including provisions around data privacy, incident response and the vendor's overall cyber security and privacy practices.
- 5.2. The board shall include cyber security, cyber safety and privacy requirements in technology procurements to ensure appropriate levels of information and user protection are in place.
- 5.3. The board shall institute cyber risk assessment practices as a key step in procurement of technology, cloud services and IT services to ensure adequacy of cyber security, cyber safety and privacy controls.
- 5.4. Contracts and service level agreements with third-party service providers (including any sub-contractors) who have access to or share custody of board information, IT systems, and/or other board technology shall include the obligation to follow the requirements of this policy and applicable board standards, procedures and guidelines, or be subject to equivalent industry-based assurances.

6. Availability and Reliability of Technology

- 6.1. The board shall define, for all business and time critical IT systems, business requirements and metrics for availability, reliability and continuity of service to inform business continuity and disaster recovery plans.
- 6.2. The board shall put in place, for all business and time critical IT systems, disaster recovery plans (DRP) to support continuity of business and timely recovery of IT systems in the event of a significant degradation of service or unplanned outage.

- 6.3. DRPs shall be the responsibility of IT and align with the Board's business continuity plan (BCP). The BCP shall help to define the business requirements for DRPs.
- 6.4. DRPs shall be periodically reviewed and maintained up to date to ensure plans can be successfully executed in the event of a disruptive event or major failure.
- 6.5. The board shall implement and periodically test backup and off-site storage procedures for all essential business information and critical IT systems no less than every 12 months, in the event data and IT systems need to be restored.

7. Network and Endpoint Security

- 7.1. The board shall implement reliable, enterprise-grade controls for the board network to regulate all traffic moving within the board network and between the board and external, untrusted (internet) entities (e.g. cloud service providers).
- 7.2. The board shall encrypt board sensitive data at rest and/or in transit as an important measure to mitigate against unauthorized access to information.
- 7.3. All board wireless access points, network connected devices, network-connected OT resources and internally or externally hosted applications (including cloud services) shall conform with board standards, procedures and guidelines.
- 7.4. Unauthorized wireless access points, connected devices, equipment, and remote connections (e.g. VPN or SSH tunnels) shall be scanned for and disabled on a regular basis.
- 7.5. The board shall not permit its networks to have open access except for managed guest networks that are isolated from the board's other network segments by reliable means.
- 7.6. The board shall implement protective measures and controls to monitor and secure endpoint devices and reduce the risk of cyber incidents and breaches from endpoint devices connected to the board network.

8. Incident and Breach Response Planning and Management

- 8.1. The board shall implement an incident and breach response plan(s) and incident and breach management procedure(s) that include definitions for metrics (e.g. severity levels, response timelines, etc.), terms used, accountability, roles and responsibilities, as well as protocols for detecting, containing, eradicating, recovering from and monitoring of cyber incidents and breaches as well as coordination, reporting, escalation procedures, and escalation contacts.

- 8.2. The board shall plan and conduct annual incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats.
- 8.3. The board shall ensure users of the board's IT and network-connected OT resources are made aware of how to identify and report a cyber incident or breach.
- 8.4. The board shall establish a process to accept and address reports of software vulnerabilities including providing a means for external reporting.
- 8.5. Any person who causes or contributes to cyber incidents or breaches shall be held accountable when their actions contravene board standards, procedures and guidelines.

9. Monitoring and Logging

- 9.1. Board networks, devices / endpoints, systems / applications, network-connected equipment and platforms shall be monitored to detect and prevent potential cyber incidents and breaches in accordance with legislation.
- 9.2. The board shall establish and maintain an audit log management process that defines the enterprise's logging requirements, including:
 - 9.2.1. Ensuring the date and time of logs is accurate by utilizing multiple authoritative time sources
 - 9.2.2. Ensuring that local logging has been enabled on critical systems
 - 9.2.3. Ensuring that logs contain adequate detail to support investigation and incident response
 - 9.2.4. Ensuring that critical systems have adequate space for the storage of log data
 - 9.2.5. Aggregating critical system logs and utilizing a a central log analytic tool (e.g. Security Incident and Event Management system) for analysis and review
 - 9.2.6. Monthly review of log analysis to identify anomalies or abnormal events
 - 9.2.7. Log and alert on critical system account audits including group changes and unsuccessful logins (e.g. Domain Admin)
- 9.3. Access to and analysis of monitoring and logging data shall be restricted to authorized personnel only.

10. Vulnerability and Patch Management

- 10.1. The board shall create and maintain an asset inventory to track the board's IT and network-connected OT assets that need security/patching and to quickly

identify, assess impacts and mitigate against vulnerabilities. The inventory shall include:

- 10.1.1. Hardware address
- 10.1.2. Network address
- 10.1.3. Machine name
- 10.1.4. Owner
- 10.1.5. Site/Department assignment
- 10.2. The board shall implement a patching and vulnerability management process to manage and mitigate board technology (software and hardware) vulnerabilities in the board's technology ecosystem. The process shall enable automatic patching for all technology or establish full vulnerability and patch management solutions to ensure technology are kept free of known vulnerabilities. Consecutive scans will be regularly compared.
- 10.3. Unauthorized assets shall be removed from the network, isolated or quarantined.
- 10.4. The board shall establish secure coding practices appropriate to the programming language and development environment being used for internally developed applications.
 - 10.4.1. For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
 - 10.4.2. The board shall ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

11. Access Control and Authorization

- 11.1. Board staff and any other individual requiring access to board sensitive information, IT systems and network-connected OT systems shall first be authorized through a board approval process. Access privileges shall be enough to enable an individual to perform their role but not permit them to exceed their authority.
- 11.2. Board user access shall be granted and/or terminated immediately upon receipt, and management's approval, of a documented access request/termination.
- 11.3. Board user accounts with elevated privileges shall be pro-actively monitored.
 - 11.3.1. Domain Administrator Accounts will be reviewed quarterly and only provisioned with the written approval of the Manager of IT.
 - 11.3.2. All users with administrative account access shall use a dedicated or secondary account for elevated activities.
 - 11.3.3. IT Services shall maintain an emergency access account with Domain Administrator privileges that requires separate secrets held by two individuals in the organization. One of these individuals shall be the

Manager of IT who shall keep their secret for emergency access off-site (break glass credential).

- 11.4. Auditing of access and usage for users' accounts shall be conducted regularly by the board to prevent privilege abuse.
- 11.5. The board shall implement multi-factor authentication (MFA) to control access to board sensitive data and systems.
 - 11.5.1. Where MFA is not possible/feasible accounts will use passwords that are unique to that system and have sufficient entropy (>80 bits)
 - 11.5.2. Where MFA is not deployed (students) the Board shall employ other technical controls (e.g. network segmentation) to prevent unauthorized access to sensitive data and systems.
- 11.6. Before deploying any new asset, IT staff shall change all default passwords to have values consistent with administrative level accounts.

12. Privacy and Data Protection

- 12.1. The board is committed to protecting the privacy of, and access to, students' and staff personal information held by the board and following rules for collection, use and disclosure as required by legislation
- 12.2. The board shall take appropriate measures to ensure the confidentiality, integrity and availability of sensitive information (including but not limited to board sensitive business information such as board financials, personal information (PI) and personal health information (PHI)).
- 12.3. All individuals with access to personal information and other board sensitive information shall be required to comply with applicable board policies, standards, procedures and guidelines, and abide by all applicable privacy laws and legislations.
- 12.4. The board recognizes the need to differentiate data from children (minors) and from that of adults, and that additional and/or different privacy safeguards may be needed for minors.

13. Cyber Awareness Training

- 13.1. The board shall conduct periodic cyber awareness training (on cyber security, cyber safety and online privacy) for authorized users of the board's IT resources and network-connected OT resources. Training shall be role-based and provide clarity on user responsibilities, where applicable in:
 - 13.1.1. Protecting board IT and network connected OT resources;

- 13.1.2. Protecting privacy and confidentiality, and complying with regulations and legislation;
 - 13.1.3. Adhering to the board's Acceptable Use of Technology AP which includes expectations of appropriate online behaviour and the safe, responsible and secure use of board technology; and
 - 13.1.4. Adhering to board Cybersecurity standards, procedures and guidelines.
 - 13.1.5. Importance of enabling and utilizing secure authentication.
- 13.2. Training shall be updated annually to address new technologies, threats, standards and business requirements.

14. Exceptions

- 14.1. The board shall develop an exception request process that ensures any deviations to the policy and standards are remediated with an established timeframe. These exception requests shall be made to the Manager of IT and reviewed by the Manager of IT, Superintendent with responsibility for IT and Senior Administration as appropriate.
- 14.2. Deviations from established cybersecurity controls shall be documented by the Manager of IT and reviewed with the Superintendent with responsibility for IT and Senior Administration as appropriate.

15. Contact

The main contact for the Cybersecurity Handbook is the Board's Manager of Information Technology.

Sean Heuchert
sheuchert@pvnccdsb.on.ca
705-748-4861 ext 1298

Any reporting for an actual or potential cyber incident should be made to the Board's IT Services Helpdesk:

helpdesk@pvnccdsb.on.ca
705-748-4861 ext 1281

Appendix A - Glossary

Access Privileges: authorized and controlled access to an information system from a pre-determined classification of set privileges, usually assigned by role (role-based access) or individual user (identity-based access).

Assets: Those resources (hardware, software, data etc.) associated with the creation, storage, processing and communication of information in the form of data, text, image or voice (i.e. Information assets, infrastructure assets and business application assets).

Asynchronous learning: Learning that is not delivered in real time. Asynchronous learning may involve students watching pre-recorded video lessons, completing assigned tasks, or contributing to online discussion boards.

Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

Availability: The degree of readiness expected of information systems and IT resources to deliver an appropriate and timely level of service, regardless of circumstances.

(Technology) Baselines: a more operationally focused form of a standard. The baseline defines a minimum level of Cybersecurity that must be met. For example, a board may choose one collaboration platform as its standard for all staff and educators. The IT department would subsequently configure this platform to a minimum baseline that ensures security and administration features are set to protect the platform.

Board Sensitive Information: Refers to school board data that must be protected from unauthorized access. It includes personal and confidential information about students and staff, and other board information such as financial data.

Breach: An information, security or privacy breach that compromises the confidentiality, integrity or accessibility of information or information systems

Business Continuity Plan: An action plan that defines alternate processes and facilities that would be used to enable critical information systems and resources to continue with planned degrees of interruption or essential change.

Cloud Service: A specific service offering and computing, networking, application, or storage function made available to users on demand via the Internet from a cloud service provider as opposed to being provided from an organization's own on-premise servers and equipment.

Confidentiality: Ensuring that information is accessible only to those authorized to have access. Unauthorized access to or disclosure of the information constitutes a loss of confidentiality. The protection of confidentiality must be consistent with the sensitivity of information and legislative requirements (e.g., MFIPPA, PHIPA).

Cyber Risk: a measure of the extent to which an entity is threatened by a potential circumstance or event, typically calculated by a consideration of the adverse impacts that would arise if a circumstance/event occurs, as well as the likelihood of it occurring.

Cyber Risk Management: is the ongoing process of identifying, assessing, and responding to risk associated with technology, the internet and the reliance on digital processes and services to run the business.

Cyber Safety: Impacts the human side and relates to safe practices to mitigate against inappropriate use and conduct online. This is especially important in the K-12 education sector.

Cybersecurity: Cybersecurity consists of standards, processes, procedures and tools organizations use to protect computers, servers, devices, networks, applications, IT systems, software and information from cyber threats, cyber threat actors, malicious cyberattacks and unauthorized access.

Cyber Threat: A cyber threat is a circumstance or event with the potential to adversely impact or compromise the security of an organization's IT systems and digital information. Examples include unauthorized access, destruction, disclosure, modification of information, and/or denial of service or system outages.

Cyber Threat Actors: A cyber threat actor are states, groups, or individuals (some very well organized and well-funded) who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to IT systems in order to access or otherwise affect victims' data, devices, systems, and networks.

Disaster Recovery Plan: Detailed steps necessary to recover information, information systems and resources at an alternate site.

Endpoint Device: general term that refers to any network-connected hardware device (e.g. smartphone, laptop, Internet-of-Things (IoT), etc.).

Elevated Privileges: Enhanced rights and/or administrative control, assigned to a user, over a particular IT resource or class of resources.

Information Technology (IT) System: is defined as any electronic system that stores, processes, or transmits information.

Integrity: The quality of authenticity, accuracy and completeness for data, which can be adversely impacted by unauthorized or accidental additions, changes and/or deletions.

Mitigate: A term related to risk management meaning the reduction of the severity of the impact or likelihood of a risk or an event.

Monitor: The process of collecting and analyzing information, on a regular basis, to check, supervise, observe critically, or track/record the progress of an activity, action, program or system towards desired outcomes.

Operational Technology (OT): Refers to network-connected equipment (hardware and software) used to change, monitor, or control physical devices and equipment such as building management systems, building automation systems, facilities sensors, HVAC (Heating, Ventilation and Air Conditioning) systems and SCADA (Supervisory Control and Data Acquisition) systems.

Personal Information (PI): MFIPPA defines personal information as recorded information about an identifiable individual. It includes information such as name, address, phone number, school photos, videos, health information and student records.

Privacy Breach: (as defined by MFIPPA) Means an incident where personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with personal information protection requirements in statute and regulation.

Privacy protection: Related to measures implemented to protect personal information from unauthorized access.

Procedures: Detailed step-by-step documents that describe the exact actions necessary to implement and/or operate specific Cybersecurity mechanisms, controls or solutions. Procedures are typically process or system specific and ensure the integrity of the process / system. Some organizations may refer to these as Standard Operating Procedures (SOPs), Administrative Procedures or other name. Some organizations may have different categories of procedures and different approval levels for each category.

Remote learning: Learning that occurs when classes are taught at a distance and when students and educators are not in a conventional classroom setting. Remote learning takes place in times of extended interruption to in-person learning – for example, as a result of a pandemic or natural disaster. Classes can be synchronous or asynchronous and can be taught online through a Learning Management System (LMS) or by using videoconferencing tools. In some cases, they may be delivered through emails, print materials, broadcast media, or telephone calls. *Definition from PPM 164¹*

Safeguard: A protective and precautionary measure intended to prevent a cyber threat from happening or a threat agent from causing harm and injury.

Significant Change: A significant or major change are those that have the potential to impact either many users or a critical board service or business function, either as part of the change implementation or as a result of a high-risk change failure.

Standards: A specification for hardware and software solutions, or mandatory requirements or actions (as may be documented in processes and/or procedures). For example, board-provided devices may have standard images that include prerequisite software and setup/configurations. Educators may be required to use specific applications when teaching in the classroom such as Microsoft Teams, Google Classroom, Zoom and other education technology tools. These may also need to be configured with specific parameters to ensure protection of privacy and mitigation of online threats.

Synchronous learning: Learning that happens in real time. Synchronous learning involves using text, video, or voice communication in a way that enables educators and other members of the school- or board-based team to instruct and connect with students in real time. Synchronous learning supports the well-being and academic achievement of all students, including students with special education needs, by providing educators and students with an interactive and engaging way to learn. It helps educators provide immediate feedback to students and enables students to interact with one another. *Definition from PPM 164²*

¹ <http://www.edu.gov.on.ca/extra/eng/ppm/164.html>

² <http://www.edu.gov.on.ca/extra/eng/ppm/164.html>

Technology Ecosystem: The collection of technology solutions that an organization uses to run its business. This includes but is not limited to computers, servers, mobile devices, networks, applications, information systems, software, education applications and tools, the internet, internet connected equipment (e.g. IoT), and digital information.

Appendix B - References

PVNCCDSB Administrative Procedures Related to Cybersecurity

Directional Policy 300 - Student Achievement and Well-Being

AP 313 - Student Acceptable Use of Technology

AP 314 - Personal Network Devices

AP 322 - Digital Privacy

Directional Policy 500 - Employee Relations

AP511 - Employee Acceptable Use of Technology

AP516 - Use of Electronic Communications and Social Media

Directional Policy 600 - Stewardship of Resources

AP 610 - Purchasing

AP 615 - Emergency Management and Business Continuity Program

AP 602 - Cybersecurity

Recommended Action:

that the Policy Development Committee recommend to the Board that Administrative Procedure #803 Pediculosis in Schools, received and posted under Directional Policy #800, Healthy Schools and Workplaces; and
that Administrative Procedure #316, Pediculosis in Schools, be deleted.



BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure	Administrative Procedure Number
Pediculosis in Schools	AP -803
Directional Policy	
800 – Healthy Schools and Workplaces	

Title of Administrative Procedure:

Pediculosis in Schools

Date Approved:

November, 2022

Projected Review Date:

2027

Directional Policy Alignment:

This Administrative Procedure aligns with the Healthy Schools and Workplaces Directional Policy 800. The Board recognizes that the health and well-being of our students and staff is foundational to their success. A healthy environment involves being respectful of one another’s social, emotional, spiritual and physical well-being. We all have a collective responsibility to create healthy work environments to keep our students and staff safe.

Alignment with Multi-Year Strategic Plan:

The Pediculosis Administrative Procedure supports the Board’s Mission to educate students in faith-filled, loving, safe, inclusive schools to develop the God-given abilities of each person. This Administrative Procedure aligns with the Board’s Multi-Year

Strategic Plan to Value Relationships, Nurture Mental Health and Well-being and to Ensure Equity.

[PVNCCDSB Board Vision, Mission and Strategic Priorities](#)

Purpose:

This administrative procedure is intended to support schools, parents/guardians and other members of the school community to understand Pediculosis and its related impact on the individual and wider community. This procedure provides for an awareness and recognition of Pediculosis and an overview of multi-layered approaches to support students, staff and families within school communities.

Action Required:

The Peterborough Victoria Northumberland and Clarington Catholic District School Board is committed to a partnership with parents/guardians, students, staff, and the school community in understanding and managing pediculosis (head lice), with dignity and compassion for all. The Board recognizes that pediculosis is not a reportable disease under the Health Promotion and Protection Act. It is defined by public health organizations as a nuisance, not a disease.

According to the [Canadian Pediatric Society: A Clinical Update \(2018\)](#),

- pediculosis infestations are not a primary health hazard or a vector for disease, but they are a societal problem with substantial costs;
- definitive diagnosis of head lice infestation requires the detection of a living louse;
- research indicates that head lice is frequently misdiagnosed and overdiagnosed, particularly when relying on nit detection only; without microscopy, the ability to distinguish viable from nonviable nits is difficult;
- when a live louse is detected in a student's head, a full course of treatment and avoiding close head-to-head activities are recommended.

According to the Canadian Pediatric Society, well-established treatment options for a proven head lice infestation include topical insecticides and oral agents. Non Insecticidal products that have been approved by Health Canada can all be obtained over the counter.

The treatment and eradication of pediculosis is ultimately parents/guardians'

responsibility; however, the school will provide information to guide them in their options.

According to the CPS, families of students in the same classroom as a student who has pediculosis must be alerted, and information on diagnosis and management should be shared with those parents as well. The dignity and privacy of all parties must be maintained at all times. Messaging that pediculosis is a common nuisance, not a disease risk or a sign of a lack of cleanliness, is important.

Ultimately, education for staff, students and parents/guardians around pediculosis detection and management is the key factor in reducing outbreaks in schools.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment of this administrative procedure with the Healthy Schools and Workplaces Directional Policy;
- Reviewing this administrative procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Providing leadership and designating resources to ensure the implementation of and compliance with this administrative procedure.

Superintendents are responsible for:

- Supporting principals and other employees for whom they have supervisory responsibility with the implementation and compliance with the procedures and requirements under this administrative procedure;
- Collaborating with the public health units within the jurisdiction of the Board to ensure updated educational materials are available to schools.

Principals and Vice-Principals are responsible for:

- Implementing this administrative procedure in accordance with the parameters outlined.
- Providing leadership and support for staff in their knowledge, understanding, and implementation of this administrative procedure.
- Creating a school action plan to respond to cases of head lice, which ensures that the dignity, privacy and well-being of students is prioritized, and which

outlines school and classroom practices which control the spread of pediculosis, to include:

- an annual regular procedure for informing parents about pediculosis, using information from Board administrative procedures and local health units (see Appendix A - *Pediculosis Fact Sheet*) for insertion on the school website, as well as in newsletters, the student agenda, etc.;
 - informing parents of potential screening options for pediculosis;
 - a process for educating staff on pediculosis to avoid misdiagnoses;
 - a clear re-admission procedure in alignment with this administrative procedure;
 - reinforcement that reporting head lice is encouraged and that confidentiality will be maintained;
 - communication throughout the year reminding parents to check their children's hair regularly for head lice and nits.
- Establishing guidelines for trained screeners in monitoring and checking students for head lice within the school. If desired, external professional services may be used for regular screening, at the school's expense.
 - Communicating with a parent/guardian when a student is identified as having pediculosis and requesting that the student be treated as soon as possible. If possible, the parent/guardian should pick up the student to initiate treatment. If this is not feasible, staff should promote preventative practices to avoid further infestation;
 - Providing a letter to the affected student's family, outlining the expectation that the student may return to class only when treatment has been administered (Appendix B), and a signed *Verification of Treatment for Pediculosis* (Appendix C) has been submitted to the school;
 - Providing written instructions for treatment, which are included in the *Pediculosis Fact Sheet* and in the *Verification of Treatment for Pediculosis* form, to the family of each identified student;
 - Ensuring that the student who returns to school after having lice is indeed lice free;
 - Sending the *Letter of Attention* (Appendix D) home to all parents of students in the class where there is a live case. If multiple cases are found during a short time frame (i.e. two-three week period), the principal will determine the number of times the letter is sent home;

- Prioritizing and preserving the affected child's well-being and dignity;
- Being culturally responsive when supporting students and families through occurrences of pediculosis.

Staff are responsible for:

- Ensuring they are knowledgeable about the requirements and parameters outlined in this administrative procedure;
- Being aware of the signs and symptoms of lice infestation;
- Reporting infestation of head lice to the principal;
- Actively promote preventative practices to avoid further infestation;
- Distributing communication materials as per the Principal's direction
- Prioritizing and preserving the affected child's well-being and dignity;
- Being culturally responsive when supporting students and families through occurrences of pediculosis.

Parents/Guardians are responsible for:

- Being aware of the signs and symptoms of lice infestation;
- Checking their children regularly for lice and/or nits, but specifically when the school has notified parents that their children may have come into contact with pediculosis;
- Reviewing with their children strategies to avoid pediculosis, such as no sharing of hats, combs or brushes, and no head-to-head contact;
- Reporting suspected cases of pediculosis to the principal;
- Arranging for their children to be picked up from school as soon as possible, and commencing treatment, should they be contacted by the school to indicated that lice have been found in their children's hair;
- Treating their children in accordance with the Public Health Guidelines and the *Verification of Treatment for Pediculosis* parameters;

- Ensuring treatment for head lice is complete, prior to returning to school;
- Completing the *Verification of Treatment for Pediculosis* form provided by the school (Appendix C), indicating the treatment which has occurred, and returning this form to the school when the children are ready to return.

Progress Indicators:

- Increased awareness within the school community, of the signs, symptoms and treatment of pediculosis through communication and distribution of public health materials to the school community;
- Processes within the administrative procedure are adhered to in support of students, staff and families and to mitigate a lice infestation within the school environment.

Definitions:

Pediculosis / Head Lice - Pediculosis/head lice are tiny insects that live only on the scalp of human beings. They do not have wings so they cannot fly or jump, and they are not found on cats, dogs, or any other household pet. The bites from head lice can cause itching and scratching. Scratching may cause sores, which may get infected.

Nits- Nits are the eggs that head lice lay. Live eggs can range in colour from off-white to dark brown, and can also be the colour of the hair they are on. Nits are typically half the size of a pinhead but they can be smaller or larger. They stick to the hair and do not fall off if touched. After the eggs are hatched, the shells are white. These empty shells stay on the hair as the hair grows.

References:

[Caring for Kids](#)

[Canadian Pediatric Society: A Clinical Update \(2018\)](#)

[Peterborough Public Health](#)

[Sick Kids About Kids Health](#)

APPENDIX A - Pediculosis Fact Sheets

(Current fact sheets provided by the Public Health units in the Board's jurisdiction.)

APPENDIX B - Letter of Notification of Suspected Head Lice

APPENDIX C - Verification of Treatment for Pediculosis

APPENDIX D - Letter of Attention to Classes of Identified Students



FACTS

About...



HEALTH DEPARTMENT



Pediculosis (Head Lice)

What is it?

Head lice are tiny insects that live on the scalp of humans. Head lice can be found on the hair very close to the scalp, behind the ears, back of the neck or behind the bangs. The saliva from head lice may cause itching. Head lice are a nuisance, but rarely cause health problems. They have nothing to do with lack of cleanliness.

How is it spread?

Anyone can get head lice. They are very common among school-aged children or children attending day care. They spread mainly through direct head-to-head (hair-to-hair) contact or through indirect contact from items such as shared hats, combs, hairbrushes, hair accessories and headphones. Lice cannot fly or hop, but they crawl very quickly. Head lice do not live on pets, such as cats and dogs.

What do I look for?

- The first symptoms are itching and scratching of the head. Some people do not itch at all. • Scratch marks may be seen on the neck and scalp and may look like a rash. • Adult lice are greyish-brown in colour and the size of a sesame seed. They move fast and are hard to see.
- Lice eggs (nits) are easily seen and will be firmly attached to the hair shaft close to the scalp. • Nits are grayish-white in colour and oval in shape.
- Nits may look like dandruff but are not easily removed.
- Nits hatch in 9-10 days and lice can survive for 1-2 days away from the scalp.

over . . .

For more information

Durham Region Health Department

905-666-6241 1-800-841-2729 durham.ca

If you require this information in an accessible format, contact 1-800-841-2729.



Pediculosis



Where to look and how to check:

- Wet the hair.
- Comb the hair with a lice removal comb (small fine-toothed comb, available at a local drugstore). • Submerge the comb into a white bowl of water.
- Look for lice at the bottom of the bowl; nits may also be seen floating in the bowl. • Examine the hair near the scalp as nits may be stuck to the hair shaft.
- Live lice may be seen in the hair, especially near the ears and neckline.
- Check all household members.

How is it treated?

- Treating head lice may require two treatments, applied about 1 week apart, to kill newly hatched lice.
- After the second treatment, check the head every 2 to 3 days for 2 to 3 weeks to ensure all lice and nits are gone.
- Head lice products can be purchased without a prescription at the drugstore. It is important to use the product as directed.
- Treatments are generally safe but for children under 2, those with allergies or women pregnant or breastfeeding, it is best to check with your health care provider or pharmacist. • Treat all those affected in your household at the same time.
- If your child has head lice, be sure that his/her school or day care is aware so that the parents can check their children. Also, tell the parents of your child's playmates.
- Wash bedding, clothing and personal items used within the last 2 days before treatment starts in hot water and dry in a hot dryer for at least 45 minutes. The heat of the water or a hot drying cycle will kill any live lice and nits.
- Personal items (such as stuffed toys) that cannot be exposed to heat should be dry-cleaned or stored in air-tight plastic bags for 2 weeks.
- Children with head lice should be treated and then attend school or child care as usual.

How can I protect myself?

- Teach children not to share combs, brushes, hair accessories, hats and headphones. • Talk to your child about avoiding head to head (hair-to-hair) contact.
- Long hair should be tied in a ponytail.

December 27, 2019

For more information

Durham Region Health Department

905-666-6241 1-800-841-2729 durham.ca

If you require this information in an accessible format, contact 1-800-841-2729.

APPENDIX B - Letter of Notification of Suspected Head Lice

(SCHOOL LETTERHEAD)

Date

Dear Parent/Guardian:

Head lice (pediculosis) have been found in your child's hair. Head lice are no reflection on the state of cleanliness; they are a recurring problem which can affect anyone in direct contact. Students are more prone to getting pediculosis because they are more likely to be in head-to-head contact.

Head lice are not a medical concern, but they are a significant nuisance for families, and need to be treated to control the spread to others. An approved treatment must be used before your child may return to school; please see the enclosed *Verification of Treatment for Pediculosis* form, which outlines the parameters required for appropriate treatment. Confidentiality for your child will be respected.

You are requested to:

- (1) read the enclosed *Pediculosis Fact Sheet*;
- (2) consult with a pharmacist or other appropriate professional about the best product to use to kill the lice;
- (3) remove all lice and nits (wet-combing with a very fine-toothed comb is effective);
- (4) complete and sign the attached *Verification of Treatment for Pediculosis* form and return it to the school office.
- (5) return with your child to school when treatment has been successfully completed.

We thank you very much for your prompt attention in this matter and for your cooperation.

Sincerely,
Principal

APPENDIX C - Verification of Treatment for Pediculosis (SCHOOL LETTERHEAD)

Verification of Treatment for Pediculosis

An approved treatment must be used before your child may return to school, as follows:

STEP ONE

I have read the information provided.

Yes No

I have used an approved head lice treatment.

Yes No

Type of treatment used:

I have removed all lice and/or nits (eggs).

Yes No

I have checked all family members, including adults, and treated if necessary.

Yes No

At successful completion of Step 1, your child may return to school. Continue with Step Two.

STEP TWO

I will be doing a daily head check for the next 10 days.

Yes No

I have planned a repeat treatment after 7 days to kill any newly hatched lice.

Yes No

I will be advising close contacts that my child has pediculosis.

Yes No

Parent/Guardian Signature: Date:

APPENDIX D - Letter of Attention to Classes of Identified Students

(SCHOOL LETTERHEAD)

Date

Dear Parent/Guardian:

Your child **may have** come into contact with head lice (pediculosis). Please check your child's head for live lice. Head lice are no reflection on the state of cleanliness; they are a recurring problem which can affect anyone in direct contact. Students are more prone to getting pediculosis because they are more likely to be in head-to-head contact. Head lice are not a medical concern, but they are a significant nuisance for families, and need to be treated to control the spread to others.

If you find head lice, please inform the principal. You must administer a treatment to kill them before your child returns to school. Wet-combing with a fine-tooth comb is a technique that assists with the removal of nits and is to be employed in conjunction with a treatment to kill the lice. A student's readmission to school is contingent upon the Parent/Guardian submitting a completed and signed *Verification of Treatment for Pediculosis* form, communicating that treatment for pediculosis (head lice) has been administered, and was successful.

Those parents/guardians of the students found to have head lice will be contacted and advised to follow the treatment outlined in the *Verification of Treatment for Pediculosis* form. Students may return to school once treatment has been completed successfully.

Please call the school with any questions,

Sincerely,
Principal

Recommended Action:

that the Policy Development Committee recommend to the Board that Administrative Procedure #1302, Bus Operator Contracted Services, be received and posted under Directional Policy #1300, Student Transportation; and

that Board Policy #1302, Bus Operator Contracted Services, and the corresponding Administrative Procedure #1302, be deleted.



BOARD ADMINISTRATIVE PROCEDURE	
<i>Administrative Procedure</i> Bus Operator Contracted Services	<i>Administrative Procedure Number</i> 1302
<i>Directional Policy</i> 1300 – Student Transportation	

Title of Administrative Procedure:

Bus Operator Contracted Services

Date Approved:

November, 2022

Projected Review Date:

2027

Directional Policy Alignment:

The Peterborough Victoria Northumberland and Clarington Catholic District School Board is aligned with Directional Policy 1300 Transportation as the Board is committed to supplying safe and effective transportation to students through contracted services with bus operators.

Alignment with Multi-Year Strategic Plan:

This administrative procedure aligns with our strategic priorities by ensuring that our contractual relationship with each of our bus operators is transparent, maintains public trust, and is fiscally responsible.

[PVNCCDSB Board Vision, Mission and Strategic Priorities](#)

Action Required:

This administrative procedure provides guidance relating to the following processes supporting the Board's relationship with its contracted bus operators, as administered through Student Transportation Services of Central Ontario:

- payment to bus operators,
- procurement of bus routes,
- limitations on holding of bus contracts,
- bus insurance,
- inclement weather and strike action affecting bus contracts,
- transfer of bus contracts,
- bus safety checks,
- vehicle/route inspections,
- maximum age of vehicles, and
- two-way communication.

As a minimum, contract agreements shall address the following items:

1. Payment to Operators

- Payment to operators, in consideration of transportation services provided, will be a monthly amount determined as ten percent (10%) of the total contract price for each route. Payments for the first few months of the school year will be based on estimates, with reconciliations and final monthly payments determined after student count dates as noted in the contracts.

2. Procurement of Bus Routes

- The Transportation Authority and Superintendent responsible for transportation will, when required or requested, meet with representatives of all school bus operators serving the Board to discuss and negotiate contract issues that arise during a contract term, or while a new contract term is being entered into.

- In accordance with the Broader Public Sector Procurement directives, a competitive procurement process may be developed in order to secure transportation services.
- When new regular daily bus routes are required to be established in the ordinary course of a school year they may be offered to an existing bus operator with capacity. Failing that, the new routes may be offered for public tender.
- Contracts will be reviewed prior to expiry of a term in order to assess where changes and/or improvements may result for future terms. Student Transportation Services officials shall advise the Board of contracts that, due to contract performance issues, should not be considered for renewal for the upcoming contract term.
- The term of existing contracts may be extended when a public procurement process is not contemplated for a renewal period. In those circumstances, existing contracts may be discontinued at the renewal date upon the following conditions:
 - (i) if the Board is dissatisfied with the services being received from the present operators, or
 - (ii) if there is a substantial change in bus routes due to population shifts, etc., and the Board wishes to reach a satisfactory new agreement with the existing operator, or
 - (iii) if it is considered that the Board is paying more than is justified for a particular route and is unable to agree on a satisfactory adjustment with the existing operator.

3. Limitation on holding of bus contracts

- It is an objective of the Board to achieve or maintain a limit on the number of bus routes to be serviced by one (1) operator at twenty-five percent (25%) of the total number of routes administered by the Board, and a limit on the amount to be paid to any one (1) operator at twenty-five percent (25%) of total transportation costs. It is to be expected that this limit will be approached gradually through the process of attrition applied to the entire bussing system.
- Approval will not be granted to award additional routes or transfer existing contracts to operators if it will result in any one (1) person or entity, or their affiliates, directly or indirectly holding contracts for more than twenty-five percent (25%) of the total number of routes administered by the Board, or which total more than twenty-five percent (25%) of total transportation costs.
- Notwithstanding the foregoing, the Board of Trustees, in its absolute discretion, may grant exceptions to this Policy in respect of any particular contract if it is of the view that it is in the best interests of the Board to do so.

- If any one (1) person or entity, or their affiliates, presently doing business with this Board, directly or indirectly, holds contracts for more than twenty-five percent (25%) of the total number of routes administered by the Board, or which equal more than twenty-five percent (25%) of the total transportation costs of the Board, that person or entity and their affiliates will not be allowed to acquire new routes until they come within the percentage requirements noted above.
- Notwithstanding the foregoing, the Board of Trustees, in its absolute discretion, may grant exceptions to this Policy in respect of any particular contract if it is of the view that it is in the best interests of the Board to do so.

NOTE FOR CLARIFICATION: An example of an ultimate owner, major shareholder or holding company is if company X is purchased by company Y but still operates under the name of company X, and, if company X holds contract at or in excess of twenty-five percent (25%), company Y would not be allowed to acquire routes under the company Y name or under any other name. The contracts held by the holding company are deemed to be those of the parent company or major shareholder thereof.

- When a public procurement process is contemplated for securing new transportation contracts, any changes to the percentages noted above will be considered by the Board prior to issuing a tender or Request for Proposal.

4. Bus Insurance

- A certificate of the insurance being carried by the contracted operator is to be filed with the Transportation Authority prior to the first day of operation in a given school year.
- All contracts will contain a clause acceptable to legal counsel for the Board, administration, and the Chief Administrative Officer requiring the operator to maintain sufficient general public liability and property damage insurance with a reputable insurance company authorized to transact business in Ontario, against claims arising out of operation of a public vehicle according to the Public Vehicles Act and the Regulations thereunder, and which insurance shall name the Board as an additional named insured.
- The limits of insurance to be carried will be specified in the actual contract agreements and will reflect both Ministry requirements and industry recommended levels.

5. Inclement Weather and Board Strike Action Affecting Bus Contracts

- When any bus route service is temporarily canceled by the Boards, including for inclement weather, the operator shall receive compensation in keeping with provisions contained within the annual Contract Agreement between Board and operator.

- In the event of a Peterborough Victoria Northumberland and Clarington Catholic District School Board strike and/or lockout whereby transportation services are cancelled, payment shall be in accordance with the following:

Number of Days Cancelled Daily Rate

6 - 15 days 85% of the per diem

16 - 35 days 75% of the per diem

36 days & over 50% of the per diem

(per diem calculated by the annual rate divided by the number of school days in the school year)

- In the event of an operator job action, no payment shall be made.

6. Transfer of Bus Contracts

- In order to deal expeditiously with requests for transfer of school bus contracts, the Chairperson of the Board and the Director of Education, or designate, are authorized to grant such request up to a maximum involvement of five (5) routes, subject to the limitations on holding bus contracts as noted above.
- The transfer of bus contracts dealing with more than five (5) routes can only be approved by the full Board. The Superintendent responsible for transportation, or designate, shall submit a detailed report, including a recommendation to approve or deny the transfer request, to the Board for its review and decision.
- The Director of Education, or designate, shall ensure that the proposed new operator of the contract can provide the necessary service and is able to meet all other requirements pertaining to vehicle loading and safety for students. The Director of Education, or designate, shall also determine the ultimate owner, major shareholders, or holding company of the proposed new operator to ensure that it is known if this new operator has contracts with the Board under any other names.

7. Bus Safety Checks

- The Transportation Authority is empowered to require any operator to have the operator's vehicle or vehicles inspected by a certified mechanic of the Board's choice or by Ministry of Transportation officials, and, if there is indeed a fault, the cost of such check will be borne by the operator; if no fault is discovered the cost will be borne by the Board.
- All vehicles used to transport students to and from school shall comply with the regulations as set down in the Highway Traffic Act and Public Vehicles Act and any other municipal and provincial laws/regulations governing their operation.

8. Vehicle/Route Inspections

- The Board recognizes the need to maintain safe bus routes and to ensure compliance with any Ministry of Education regulations. There is also a need to confirm/review distance claims, vehicle sizes, and compliance to Ministry of Transportation regulations as submitted by operators. A minimum of the Board's total bus routes and any new routes should be audited annually through field audits. These audits should focus on:
 - (a) route efficiency;
 - (b) distance claims by operators;
 - (c) visual inspection of vehicle;
 - (d) safety of pick-up and drop-off location;
 - (e) driver skills; and
 - (f) public vehicle licensing requirements.

9. Maximum Age of Vehicles

- Operators shall not use vehicles for the transportation of students that have been in service for more than twelve (12) years without the annual approval of the Transportation Authority, in writing.

10. Two-way Communication

- The operator shall, at his or her expense, purchase, arrange for, and provide all vehicles with two-way communication equipment. The equipment must:
 - be able to provide mobile-to-mobile communication as well as mobile-to-base;
 - be able to have dispatch and/or central monitoring from a location or several locations;
 - be able to communicate with a base from everywhere in the area where the operator generally operates for the Board, e.g., charter work for the Board and its schools;
 - be able to operate under adverse weather or other conditions, e.g., should hydro fail to the tower site, radio system should not be inoperative;
 - be as technically simple as possible;
 - be transferrable from one (1) vehicle to another in the event that a spare bus is being used, or spare buses be equipped with the same type of radios; and
 - have central monitoring with direct and continuous access to necessary parties to further rider safety or for dispatch of emergency services.

Responsibilities:**The Board of Trustees is responsible for:**

- Reviewing this Administrative Procedure to ensure its alignment with Directional Policy 1300 Student Transportation
- Reviewing the Bus Operator Contracted Services Administrative Procedure as part of its regular policy and procedures review cycle.
- Approving transfers of bus contracts.
- Approving exceptions to this Administrative Procedure when it is in the best interests of the Board to do so
- Approving renewals to contract terms

The Director of Education is responsible for:

- Overseeing implementation of this Administrative Procedure
- Approving bus transfers when the number of routes is less than five.

Superintendent responsible for transportation is responsible for:

- Supporting STSCO during the procurement process, and contract renewals
- Ensuring that recommendations regarding bus transfers and contract renewals are properly supported for the Board of Trustees approval.

Progress Indicators:

- Bus contract renewals or bus transfers are completed on a timely basis, with no interruption of service to students.

Definitions:

- Transportation Authority
For the jurisdictions of the Board in Peterborough, Northumberland, and Clarington, the Transportation Authority is Student Transportations Services of Central Ontario, through its Chief Administrative Officer. For the City of Kawartha Lakes, the Transportation Authority is Trillium Lakelands District School Board, through its Transportation Supervisor.

- Total Transportation Costs

Total Transportation Costs are defined as the sum total of the costs of all transportation contracts for a school year as determined on 31 October of that school year.

References:

- Ontario Public Vehicles Act and Regulations thereunder
- Ontario Highway Traffic Act and Regulations thereunder

Recommended Action:

that the Policy Development Committee recommend to the Board that Administrative Procedure #1305, Accidents Involving School Purpose Vehicles, be received and posted under Directional Policy #1300, Student Transportation; and that Board Policy #1305, Bus Accidents and Resulting Injuries, the corresponding Administrative Procedure #1305, be deleted.



BOARD ADMINISTRATIVE PROCEDURE	
<small>Administrative Procedure</small> Accidents Involving School Purpose Vehicles	<small>Administrative Procedure Number</small> 1305
<small>Directional Policy</small> 1300 – Student Transportation	

Title of Administrative Procedure:

Accidents Involving School Purpose Vehicles

Date Approved:

November, 2022

Projected Review Date:

2027

Directional Policy Alignment:

This Administrative Procedure aligns with the Directional Policy 1300 Student Transportation as it is built upon ensuring that consistent procedures are established and carried out in the event of an accident involving a school purpose vehicle.

Alignment with Multi-Year Strategic Plan:

This Administrative Procedure aligns with the multi-year strategic plan as we strive to maximize an effective and efficient student transportation system, within the resources available, while attending to student safety.

[PVNCCDSB Board Vision, Mission and Strategic Priorities](#)

Action Required:

All accidents involving a student or students and/or a contracted school purpose vehicle, no matter how minor, shall be reported to the Transportation Authority and the school or schools whose students are assigned to the vehicle.

1. In the event of an accident, the driver's first responsibility is to the students/passengers, and the driver shall:
 - Remain with the vehicle and passengers
 - Determine, as quickly as possible, if anyone is injured
 - Immediately use the onboard two-way communication device to report the accident (providing exact location to assist First Responders in locating the scene)
 - Explicitly ask for ambulance dispatch if any students/passengers are hurt or report minor injuries
 - Attend to injured students while waiting for First Responders to arrive
 - Follow direction of First Responders when they arrive
2. School staff, once notified of an accident involving students on a school purpose vehicle (regardless of whether there are injuries), are to notify parents/guardians as soon as possible and advise the parent/guardian of the accident. Where school staff is not available to contact families, the bus operator assumes the responsibility of contact.
3. Schools, where possible, should develop a mechanism to ensure staff coverage (with access to a student database) is available for the time required to contact all affected families.
4. Operators of vehicles under contract to the Board that are involved in an accident (either prior to the first pick-up or following the last drop-off) are also responsible for reporting the accident to the Transportation Authority, as the reports form part of the Contract Management system
5. Once advised, the Transportation Authority will notify the appropriate Education Centre personnel (i.e. school superintendent, Communications Services, superintendent responsible for transportation, etc.) Staff representatives of the Transportation Authority may be dispatched to attend to an accident scene as well.
6. As soon as possible after an accident, the driver will file a report with the operator using the accident report form supplied by the Transportation Authority.

(Appendix A). The operator will be responsible for supplying the Transportation Authority with a completed copy of the accident report form within twenty-four hours of the accident.

7. Accident Contact List:

In order to assist in the above processes, it is required that each bus display a listing of:

- Appropriate police telephone numbers
- Driver's name
- Bus operator name and telephone number
- Transportation Authority telephone numbers
- Transportation Authority contact personnel
- Route number
- Schools served and
- List of passengers on the route and contact telephone number of each.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment of this Administrative Procedure with the Directional Policy

The Director of Education is responsible for:

- Responding to reports of accidents and supporting the principal and school community as needed. In the event of serious injuries, will act as Board spokesperson, or delegate the responsibility as appropriate.

Superintendents of Schools and System Portfolios are responsible for:

- Responding to reports of accidents and supporting the principal and school community as needed. This may include involving the Crisis Response Team.

Principals and Vice-Principals are responsible for:

- Supporting the communication process to parents/guardians when notified of an accident.

Communication Services is responsible for:

- Communicating and providing appropriate context to the public and media in the event of a serious accident with injuries.

Transportation Authority is responsible for:

- Advising appropriate personnel at the Education Centre, in a timely manner, in the event of an accident.
- Ensuring that all information relevant to any accident is received from the bus operator for investigative and contract purposes.

Progress Indicators:

- Information and contact with school authorities and through to parent/guardians is timely.
- Data relevant to any accidents is incorporated in the annual evaluation of bus operator performance.

Definitions:

- Transportation Authority: For the jurisdictions of the Board in Peterborough, Northumberland and Clarington, the Transportation Authority is Student Transportation Services of Central Ontario, through its Chief Administrative Officer. For the City of Kawartha Lakes, the Transportation Authority is Trillium Lakelands District School Board, through its Transportation Supervisor.
- First Responders – The term “first responder” includes a firefighter, law enforcement officer, paramedic, emergency medical technician, or other individual (including an employee of a legally organized and recognized volunteer organization, whether compensated or not), who, in the course of his or her professional duties, responds to emergencies.
- School Purpose Vehicle is a vehicle contracted to provide student transportation for the Board, through a Service Provider.



ACCIDENT REPORT

ROUTE # _____

BUS COMPANY NAME _____

ADDRESS

TIME AND PLACE OF ACCIDENT	Date of Accident _____, 20__		Time _____	A.M.	P.M.	
	Accident Location _____					
	Did Police investigate?		Officer's Name _____		Number _____	
	Station of Officer _____					
	Does this accident involve bodily injury? YES <input type="checkbox"/> * see below NO <input type="checkbox"/>					
OPERATOR/ BOARD VEHICLE AND DRIVER	Make and Type _____	Year _____	Style _____	Vin. No. _____	Lic. _____	Unit # _____
	Name of Driver _____			Age _____	Driving Experience _____	
	Address _____			City _____	Prov. _____	
	Driver's Lic. No. _____			Telephone No. _____		
	While employed by your company has driver been involved in any accident within the past two years?					
	For what purpose was vehicle being used? <input type="checkbox"/> School Route <input type="checkbox"/> Field Trip <input type="checkbox"/> Other					
	Any indication of charges by Police? _____					
OTHER VEHICLE	Make and Type _____	Year _____	Style _____	Lic. _____	Prov. _____	
	Name of Owner _____			Address _____		
	Name of Driver _____			Address _____		
	Insurance Company _____			Policy Number _____		
	Description of Damage _____					
	Statement of Driver (if any) _____					
	*NOTE - if more than one vehicle involved, use supplementary sheet					
	Any indication of charges by Police? _____					
PROPERTY DAMAGE OTHER THAN VEHICLE	Describe damage in detail: _____					
	Owner _____			Address _____		
* STUDENT INJURIES <small>(Attach list if necessary)</small>	Name _____			Address _____		
	Nature and extent of injury _____					
	Injury occurred <input type="checkbox"/> On Board <input type="checkbox"/> Outside of Bus					
	Taken home or to hospital _____					
	Statement of injured person after accident _____					
* OTHER INJURIES <small>(Attach list if necessary)</small>	Name _____			Address _____		
	Nature and extent of injury _____					
	Injury occurred <input type="checkbox"/> On Board <input type="checkbox"/> Outside of Bus					
	Taken home or to hospital _____					
	Statement of injured person after accident _____					

ALL PASSENGERS ON BOARD AT TIME OF ACCIDENT: (ATTACH LIST IF NECESSARY)

NAME	ADDRESS	PHONE



DRIVER'S REPORT OF ACCIDENT:

Weather Conditions (check appropriate boxes)	Road Conditions	Light Conditions
1. No Adverse Conditions <input type="checkbox"/> 2. Rain <input type="checkbox"/> 4. Fog <input type="checkbox"/> 3. Snow <input type="checkbox"/> 5. High Wind <input type="checkbox"/>	1. Dry <input type="checkbox"/> 4. Ice <input type="checkbox"/> 2. Wet <input type="checkbox"/> 5. Dirt <input type="checkbox"/> 3. Snow <input type="checkbox"/> 6. Sand <input type="checkbox"/>	1. Daylight <input type="checkbox"/> 4. Dark <input type="checkbox"/> 2. Dawn <input type="checkbox"/> 5. Street light <input type="checkbox"/> 3. Dusk <input type="checkbox"/> 6. Other <input type="checkbox"/>

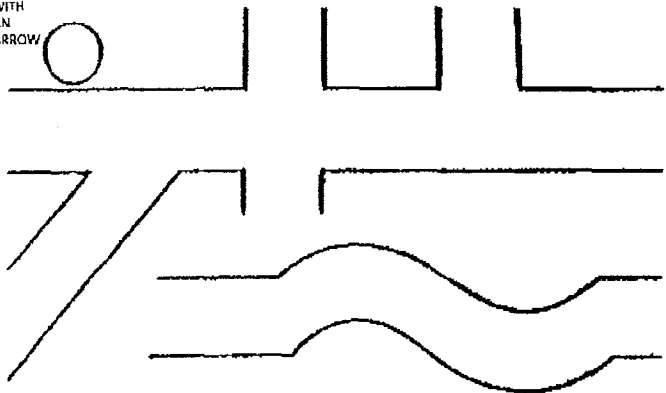
EMPLOYEE/DRIVER DESCRIPTION OF ACCIDENT:

DIAGRAM OF ACCIDENT SCENE:

INSTRUCTIONS:

- Choose sections of diagram that will show outline of roadway at place of accident.
- Use solid line to show path of vehicle BEFORE accident
dotted line AFTER accident
- Number each vehicle and show direction of travel by arrow:
- Show PEDESTRIAN by: ----- ○
- Show RAILROAD by: ----- 
- Show TRAFFIC LIGHT by: ----- 
- Show STOP SIGN by: ----- ◇
- Indicate distance and direction from point of interest to nearest bridge, culvert or other landmarks.
- Indicate names of streets or route numbers of roadways.

INDICATE NORTH WITH AN ARROW



Driver Signature _____

Date: _____

Company Investigator: Name: _____

Signature: _____

Investigators Comments: Non-Preventable Preventable
