ST. CLAIR CATHOLIC DISTRICT SCHOOL BOARD
POLICIES AND PROCEDURES
SECTION B: ADMINISTRATION

PRIVACY	PROCEDURE
EFFECTIVE: 2017 04 25	

APPLICABLE REFERENCES:

Legislation

- Education Act, Ontario: s266; and s171(38)
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA); 2004 C. 3 Sch. A
- Personal Information Protection and Electronic Documentation Act (PIPEDA)
- Immunization of School Pupils Act, 1990

Other Related

- Information and Privacy Commission of Ontario http://www.ipc.on.ca/
- The Ontario Student Record Guideline
- The Ontario School Boards and Authorities Privacy Standard
- Office of the Privacy Commissioner of Canada: Youth Privacy
- Sec B: Policy - Privacy
- Sec B: Policy - Freedom of Information and Protection of Privacy Act (FIPPA)

ADMINISTRATIVE PROCEDURES:

The Board supports the protection of individual's rights to privacy regarding their *personal information* (see definition in 4.0) and compliance with all applicable provisions of legislation and related regulations related to the collection, use, retention and disclosure of personal information.

The board may access personal information data, files or records available in or via its systems during the course of its normal routines or responsibilities.

1.0 Responsibility

1.1 The Director of Education and/or designate is accountable for the Board's compliance with privacy legislation and will be the accountable decision maker in responding to privacy breaches in accordance with this procedure.

1.2 The Treasurer of the Board will be responsible for the implementation of this policy and procedures.

1.3 The staff member assigned the duty of Privacy Officer will ensure Senior Administration, Managers and Principals are informed of their legislative responsibilities for the collection, use, retention and disclosure of the personal information of staff and students in accordance with this procedure.

1.4 Senior Administration, Managers and Principals will be responsible for communicating this procedure to all individuals involved in the collection, use, retention and disclosure of the personal information of staff and students.

2.0 Expectations

2.1 Senior Administration understands that:

2.1.1 Under MFIPPA, the Board is responsible for personal information under its control and may designate an individual within the school board to be accountable for compliance with privacy legislation.

2.1.2 Under PHIPA, health information custodians are responsible for personal health information and the Board may designate an individual within the school board to assist with privacy compliance.

2.2 Human Resource Services will:

2.2.1 Ensure that all new employees review and sign the Board's Confidentiality Acknowledgment Form (Appendix A).

2.3 Senior Administration, Managers, and Principals will:

2.3.1 Ensure that all requests for and collection of personal information are conducted only for *specified purposes* (see definition in 4.0) and are limited to what is required to execute the Board's statutory duties and responsibilities.

2.3.2 Ensure that the purposes for which personal information is collected be specified, noting the legal authority for the collection, and the title of an individual who can answer questions about the collection.

2.3.3 Ensure that except where already permitted by law, appropriate *consent* (see definition in 4.0) by an individual is obtained for the collection, use, retention and disclosure of personal information.

2.3.4 Ensure that personal information is not used for purposes other than that for which consent was obtained, unless prior consent has been obtained from the individual or as authorized or required by law.

2.3.5 Ensure that the personal information is accurate, complete and current in order to fulfill the specified purposes for its collection, use, disclosure and retention.

2.3.6 Ensure that personal information is secured and protected from unauthorized access, use, disclosure and inadvertent destruction by adhering to reasonable safeguards appropriate to the sensitivity of the information. Personal information that has been used by the Board must be retained after use for a period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to it.

2.3.7 Make available to the public specific information about the Board's policies and practices relating to the collection, use and retention of personal information.

2.3.8 Ensure that contracted third parties, who provide services that access personal information of staff or students, are aware of the Board's privacy expectations and acknowledges those requirements by completing the Privacy Requirements for Third Party Service Providers Form (Appendix B).

2.3.9 Ensure that where a privacy breach has been identified:

- All available information about the nature of the breach or suspected breach is obtained, and determine what happened;
- The Privacy Officer is alerted and provide as much information about the breach as is currently available;
- Assistance is provided to the Privacy Officer to undertake all appropriate actions to contain the breach; and
- Details of the breach and corrective actions are documented.

2.4 The Board's Privacy Officer will:

2.4.1 Ensure that the appropriate staff are informed of their legislative responsibilities for the collection, use and disclosure of the personal information of staff and students.

2.4.2 Maintain and make available to staff, the board's records retention schedule.

2.4.3 Execute the Board's Privacy Breach Protocol (Appendix C) ensuring that all five steps of the response protocol are implemented.

2.4.4 Develop and maintain the Board's Privacy Breach Protocol.

2.4.5 Process formal requests and privacy complaints in accordance with legislated and regulated process requirements.

2.4.6 Complete the annual report required by the office of the Information and Privacy Commissioner of Ontario.

2.4.7 Provide consultation and support regarding information access and privacy protection for all staff and members of the public.

2.4.8 Ensure that the Board's website includes an easily accessible Privacy Policy that aligns with this procedure.

2.5 Board employees will:

2.5.1 Review the Board's Confidentiality Acknowledgment Form (Appendix A).

2.5.2 Except where already permitted by law, obtain appropriate informed consent for the limited collection, use, retention and disclosure of personal information.

2.5.3 Endeavour to ensure that personal information is: accurate, complete and up to date; and secured and protected from unauthorized access, use or disclosure.

- Do not disclose passwords or write them down;
- Change passwords as directed by the Information Services department; and
- When sending personal information via voice or electronic messages be certain it is being sent to the correct destination and that it is secure.

2.5.4 Be alert to the potential of personal information to be compromised, and therefore potentially play a role in identifying, containing and notifying their supervisor of an actual or potential privacy breach.

2.5.5 Shall release *general information* (see definition in 4.0), where appropriate.

2.5.6 Shall release personal information to the person to whom it relates or to his/her parents, in accordance with MFIPPA.

2.5.7 Shall consult with the Privacy Officer where there is uncertainty about the accessibility of information being requested.

2.5.8 Shall refer all requests referring to MFIPPA to the Privacy Officer.

2.5.9 Shall retain personal information using secure methods for a period documented in the Board's Records Retention Schedule.

2.5.10 Shall respect an individual's right to:

- Access and have copies of their personal information, with limited exceptions;
- Request removal of or corrections to personal information; and
- Lodge a privacy complaint.

2.5.11 Shall ensure that they are aware of the Board's requirements under its Privacy Breach Protocol (Appendix C).

3.0 Additional Information

3.1 The St. Clair Catholic District School Board is committed to the principles of equity and inclusive education, consistent with our Catholic teachings, which value and promote human rights and social justice in all Board policies, programs, guidelines, operations and practices.

4.0 Definitions

Consent – Personal information is collected for the provision of educational services to students. The knowledge and, in some cases, the consent of an individual is required for the collection, use, retention and disclosure of personal information, except where otherwise permitted by law.

General Information – Information that bears no personal information or identifiable information about an individual or information that has been aggregated to indicate macro level data or observations.

Personal Information (MFIPPA: s 2.1) - Recorded information about an identifiable individual, including:

a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
b) Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
c) Any identifying number, symbol or other particular assigned to the individual,
d) The address, telephone number, fingerprints or blood type of the individual,
e) The personal opinions or view of the individual except if they relate to another individual,
f) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
g) The views or opinions of another individual about the individual, and

h) The individuals name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Specified Purposes - The school board shall identify the purpose(s) for which personal information is collected, and individuals shall be notified of the purposes and any other information required by law at or before the time personal information is collected.

APPENDIX A

CONFIDENTIALITY ACKNOWLEDGEMENT

The St. Clair Catholic District School Board (the "Board") has custody and control of confidential information that it must protect for ethical and legal reasons.

The following examples of confidential versus non-confidential information is not an exhaustive list.

Confidential Information	Non-confidential Information
• Identifiable/personal information about persons • Documents deemed to be or marked Confidential • Documents in personnel files • Disability and health information • HR, payroll and absence data • Passwords • Systems, operations and business activities	• Confirmation of employment • Name, job title, business address or business contact number(s) of an individual • High level aggregated no identifiable data • Information legitimately publicly available

As an employee of the Board, you have general and specific duties regarding the treatment of confidential information.

General Duties

1. Refrain from accessing, using, disclosing and destroying confidential information, except as specifically authorized or as is necessary to perform their work of or meet a responsibility of the Board;

2. Take reasonable precautions and care to protect confidential information from loss, theft, unauthorized access, disclosure, destruction, copying, use or modification;

3. Report loss, theft, unauthorized access, disclosure, destruction, copying or modification of confidential information to your supervisor immediately; and

4. Upon ceasing to be employed, the employee will return to the Board all confidential information in his/her possession or under his/her control as well as all Board property.

Specific Duties

1. Refrain from discussing confidential information in public or in any area where is it likely to be heard by others who are not entitled to receive the information (hallways, lunchrooms, elevators);

2. Refrain from allowing another person from using your assigned access credentials or fobs to systems and facilities;

3. Refrain from leaving confidential information unattended (desks, printers, fax machines);

4. Ensure confidential information is properly secured outside of work hours (locked in drawers, offices, filing cabinets);

5. Ensure documents and electronic files containing confidential information are not removed without appropriate authorization and are not stored on personal computers;

6. Ensure documents and electronic files containing confidential information that are removed from Board premises are properly secured; and

7. Only access, process, transmit and store confidential information using authorized hardware, software and other equipment provided by the Board. Confidential information is not be stored or transmitted using personal email accounts or unsecured media.

By signing this document, I am confirming that:

- I have read this acknowledgement and understand my duties regarding the treatment of Confidential Information.

- Should I leave the employ of the St. Clair Catholic District School Board for any reason, I further understand that my obligations with respect to the treatment of confidential information obtained through the course of my employment continue to apply.

Employee Name_____

Employee Signature_____

Date_____

APPENDIX B

PRIVACY REQUIREMENTS OF THIRD PARTY SERVICE PROVIDERS

The St. Clair Catholic District School Board collects, uses, retains and discloses personal information in the course of meeting its statutory duties and responsibilities. The Board is committed to the protection of privacy of personal information and complies with all applicable provisions in the *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act,* the *Personal Information Protection and Electronic Document Act* and any other applicable legislation and related regulations.

Personal Information (MFIPPA: s 2.1) Is recorded information about an identifiable individual, including:

a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual
b) Orientation or marital or family status of the individual,
c) Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
d) Any identifying number, symbol or other particular assigned to the individual,
e) The address, telephone number, fingerprints or blood type of the individual,
f) The personal opinions or view of the individual except if they relate to another individual,
g) Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
h) The views or opinions of another individual about the individual, and
i) The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

All third party services providers must monitor and enforce their compliance with privacy and security requirements defined in the contracts or service agreements, and are required to inform the Board of all actual and suspected privacy breaches.

The third party service providers have the responsibility to:

- Inform their Board contact as soon as a privacy breach or suspected breach is discovered;
- Take all necessary actions to contain the privacy breach as directed by the Board;
- Document how the breach was discovered, what corrective actions were taken and report back;
- Undertake a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;
- Take all necessary remedial action to decrease the risk of future breaches; and
- Fulfill contractual obligations to comply with privacy legislation.

_____

Company Name

_____

Representative (Print and Sign)

_____

Date

Please return signed copy to the Privacy Officer.

APPENDIX C

PRIVACY BREACH PROTOCOL

PURPOSE

The St. Clair Catholic District School Board is committed to ensuring the protection of personal information in its custody and control.

The following protocol outlines the necessary steps to contain and respond to incidents involving the unauthorized disclosure of personal information. Employees have a role and responsibility to assist in the containment of a privacy breach.

SCOPE

This protocol applies to all Board employees, trustees and volunteers.

DEFINITION

A privacy breach occurs when personal information is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. The Board is governed by the following privacy statutes: *Municipal Freedom of Information and Protective of Privacy Act* (MFIPPA), *Personal Health Information Protection Act* (PHIPA), *Immunization of School Pupils Act* and *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error or can involve technology/computer error. The following are some examples of privacy breaches: student report card mailed to the wrong home; hard copy psychological assessments kept in openly accessible file cabinets that are not secured or controlled; theft from a car of a briefcase containing a list of home addresses of teaching staff; lost memory/USB key containing student data; or theft from a teacher's car of a laptop containing student records.

RESPONSIBILITY/ACCOUNTABILITY

Director of Education (or designate)

- The responsibility for protecting personal information affected by a privacy breach is assigned to the Director of Education or designate who is the accountable decision maker, familiar with the Board's roles, responsibilities and the response plan.

Employees:

- All employees need to be alert to the potential of personal information to be compromised, and therefore potentially play a role in identifying, notifying, and containing a breach.
- Employees should notify their supervisor immediately, or, in his/her absence, the Board'sPrivacy Officer upon becoming aware of a breach or suspected breach.
- Employees dealing with student, employee and/or business records need to be particularly aware of how to identifying and address a privacy breach.

Senior Administration, Managers, and Principals:

- Are responsible for alerting the Privacy Officer of a breach or suspected breach and will work with the Privacy Officer to implement the five steps of the response protocol.
- Have the responsibility to:
    - Obtain all available information about the nature of the breach or suspected breach, and determine what happened;
    - Alert the Privacy Officer and provide as much information about the breach as is currently available;
    - Work with the Privacy Officer to undertake all appropriate actions to contain the breach;
    - Ensure details of the breach and corrective actions are documented

Privacy Officer:

- Ensures that all five steps of the response protocol are implemented.
- Will follow the following five steps: Respond, Contain, Investigate, Notify and Implement Change.

Third Party Service Providers:

- In many instances, the Board uses contracted third party services providers to carry out or manage programs or services on its behalf.
- Typical third party service providers are commercial school photographers, bus companies, external data warehouse services, outsource administrative services (such as cheque production, records storage, and shredding), Chatham-Kent Lambton Administrative School Services (CLASS), Children's Aid Societies (CAS), Public Health Units (PHU), external researchers, and external consultants.
- In such circumstances, the Board retains responsibility for protecting personal information in accordance with privacy legislation.
- Therefore, third party service providers need to know their roles and responsibilities if a privacy breach occurs when they have custody of personal information.
- All third party service providers must take reasonable steps to monitor and enforce their compliance with privacy and security requirements defined in the contracts or service agreements, and are required to inform the Board of all actual and suspected privacy breaches.
- The third party service providers have the responsibility to:
    - Inform the Board contact as soon as a privacy breach or suspected breach is discovered;
    - Take all necessary actions to contain the privacy breach as directed by the Board.
    - Document how the breach was discovered, what corrective actions were taken and report back;
    - Undertake a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;
    - Take all necessary remedial action to decrease the risk of future breaches;
    - Fulfill contractual obligations to comply with privacy legislation.

ACTIONS

In the case of a privacy breach or suspected breach, the Privacy Officer will implement concurrently the five steps of the response protocol.

Step 1 – Respond:

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

Step 2 – Contain:

- Identify the scope of the breach and contain it (e.g., retrieve the hard copies of any personal information that has been disclosed, determine if the breach would allow unauthorized access to any other personal information [e.g., electronic information systems], change passwords and identification numbers and/or temporarily shut down the system if necessary to contain the breach);
- Document the breach and containment activities;
- Develop briefing materials;

- Brief the accountable decision maker, senior management, and key persons on the privacy breach and how it is being managed.

Step 3 – Investigate:

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

Step 4 – Notify:

- Notify, as required, the individuals whose personal information was disclosed if it is determined that notification is required.
- The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:
    - What happened;
    - The nature of potential or actual risks or harm;
    - What mitigating actions the Board is taking; and
    - Appropriate action for individuals to take to protect themselves against harm.
- If personal information that could lead to identity theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's rights to complain to the IPC about the Board's handling of their personal information, along with contact information for the IPC.
- Notify appropriate managers and employees with the Board of the breach;
- Report the privacy breach to the office of the Information and Privacy Commissioner (IPC) as appropriate.

The following factors should be considered by the Privacy Officer when determining whether notification is required:

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

ii. *Risk of Physical Harm*

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

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

iv. *Risk of Loss of Business or Employment Opportunities*
Could the loss of theft of information result in damage to an individual's reputation affecting his/her business or employment opportunities?

Step 5 – Implement Change:

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

MAINTAIN RECORDS

- The Privacy Officer will ensure that thorough documentation of all notes taken related to the breach or suspected breach are filed according to the Board's records retention schedule.