Privacy

Date: 2015 02 24/ 2023 04 25

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. Responsibilities

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. 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) 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) 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 Ensure that employees know and honour guardian consents for use of student personal information such as names, photos, class work, etc. to be used on Board or school websites, social media sites or other external publications.

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

2.3.9 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 acknowledge those requirements by completing the Agreement for the Confidentiality and Security of Personal Information. (Appendix B).

2.3.10 Ensure that where a privacy breach is suspected or has been identified, the Board's Privacy Officer is contacted and assist with aspects of the Breach Protocol as directed.

2.4 The Board's Privacy Officer will:

2.4.1 Develop and Implement a privacy framework for the Board to identfy and manage privacy risk.

2.4.2 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.

2.4.3 Provide the privacy perspective to the board's records retention policy and procedures.

2.4.4 Develop, maintain and Execute the Board's Privacy Breach Protocol (Appendix C).

2.4.5 Process Freedom of Information 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 Understand their obligations for Privacy and sign the Board's Confidentiality Acknowledgment Form (Appendix A).

2.5.2 Honour guardian responses to the Use of Student Personal Information Consent Form before deciding to share student activity or work.

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

2.5.4 Confirm that third party applications and social media have been vetted for privacy and data security before using and familiarize themselves, prior to posting, with the security/privacy settings needed for any social media, website and web-based forums they intend to use.

2.5.5 Obtain informed guardian consent for use of classroom applications and social media that have not been sanctioned by the Board. A Template letter is provided

in Appendix D and should be modified to suit the specific needs of the activity or work.

2.5.6 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;
- Follow security protocols 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.

2.5.7 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.

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

2.5.9 Shall release personal information to the person to whom it relates or to their legal guardian, in accordance with MFIPPA.

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

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

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

2.5.13 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.

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

3. 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.

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.

References

Legislation

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

Other Related

- Information and Privacy Commission of Ontario
- The Ontario Student Record Guideline
- The Ontario School Boards and Authorities Privacy Standard
- Office of the Privacy Commissioner of Canada: Youth Privacy

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 of students/staff • 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 your work 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 (laptops, desks, printers, fax machines);

4. Follow Responsible Use of Technology Procedures to 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 devices/drives;

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 following Agreement for the Confidentiality and Security of Personal Information (amended to meet the services being provided) should be inserted/modified/requested from any third party where personal information of staff or students will be disclosed, created, stored, used or modifed:

AGREEMENT for the CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

Between

St. Clair Catholic District School Board (the Board)

and

Company Name (The Company)

WHEREAS the School Board/School wishes the Company to provide, and the Company wishes to provide the services more fully set out in the agreement between [the Company] and the [Board/School].

AND WHEREAS Such services may require the Company to have access to and/or possession of and/or use of personal information under the control of the Board, they shall be subject to the terms and conditions hereinafter set out;

NOW THEREFORE In Consideration of the mutual covenants, agreements and undertakings herein contained, the Company on behalf of itself and its successors and assigns and the Board on behalf of itself and its successors mutually covenant and agree as follows:

1. TERM. The term of this agreement shall be only for the project which the Company is working with the Board that require the Company to have access to and/or possession of and/or use of personal information under the control of the Board.

2. PERSONAL INFORMATION. The Parties recognize the application of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O., 1990, c.M-56 (MFOI/POP) and Regulations thereunder, as amended from time to time, to the collection, use and disclosure of personal information under the control of the Board.

a. For the purpose of the application of the MFIPPA/PHIPPA, the definition of personal information shall be as defined pursuant to MFIPPA/PHIPPA.
b. For the purposes of this agreement, any personal information provided/created under this agreement shall be under ownership and control of the Board.

3. COLLECTION BY COMPANY. The Parties recognize the application of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 (PIPEDA) and Regulations and Schedules thereunder, as amended from time to time, to the collection, use and disclosure of personal information by the Company for its own use and/or benefit.

a. For the purpose of the application of the PIPEDA, the definition of personal information shall be as defined pursuant to PIPEDA.

b. The Parties agree that at no time will the Company for its own use and/or benefit collect, use and/or disclose personal information about and/or belonging to students of the Board without express written approval from the custodial parent/guardian of

the student. Use of personal data will be limited directly to purposes as set out in the express consent provided by the parents.

4. WARRANTIES AND COVENANTS. Without limitation to any other provision of this Agreement, the Company represents and warrants to and covenants with the Board as follows, at all times during which the Company is providing services that may require the Company to have access to and/or possession of and/or use of personal information under the control of the Board:

a. the Company shall comply with all provisions of MFIPPA and all Board policies and procedures regarding the collection, use, disclosure and retention of personal information under the control of the Board;

b. under no circumstances shall the Company or its employees disclose personal information under the control of the Board;

c. the Company shall employ appropriate security measures, as determined by the Board in its sole discretion, to protect the confidentiality of the personal information in its possession but under the control of the Board if in the Company's possession as a result of the services being requested of the Board;

i. Security measures are determined based on current best practices in the industry (at the physical hardware level, at the server software level, and at the Company software level). The Company reviews security practices annually, performs third party security audits, and has internal training for any staff who will gain access to the production server.
ii. Understanding that the Board is responsible to ensure that the Provider has adequate system security measures, the Provider will provide, upon request, an accounting of third party security audits, results and measures being taken to address any recommendations.

d. only those employees or agents employed by the Company who require access to personal information under the control of the Board for the purpose of performing their duties with respect to the project being requested of the Board shall be provided with access to such personal information;

e. the Company shall inform the Board of all actual and suspected privacy breaches (defined as possible disclosures that the Company cannot confirm or deny have taken place, within 3 days investigation from the time of notification of the possibility of a breach) affecting personal information under the control of the Board, including inappropriate access to information by employees; The Company will work with the Board to address privacy breach protocols as identified by the Board/school in their privacy policies/procedures.

f. the Company shall either return or destroy, as determined by and in a manner to be determined by the Board in its sole discretion, any and all personal information under the control of the Board if in the Company's possession as a result of the project by the Company;

g. the Company, except as may be required by law, agrees to not use, directly or indirectly, for its own account or for the account of any person, firm, Board/School or

other entity or disclose to any person, firm, Board/School or other entity, the Board/School's secret business information disclosed or entrusted to it or developed or generated by it in the performance of its duties hereunder, including but not limited to information relating to the Board/School's organizational structure, operations, business plans, technical projects, business costs, research data results, inventions, trade secrets, or other work produced, developed by or for the Board/School, whether on the premises of the Board/School or elsewhere. The foregoing provisions shall not apply to any proprietary, confidential or secret business information which is, at the commencement of the Term or at some later date, publicly known under circumstances involving no breach of this Agreement or as lawfully and in good faith made available to the Company without restrictions as to disclosure to a third party; and

h. the Company shall at all times indemnify and save harmless the Board, its directors, trustees, members, officers, employees, agents, successors and assigns from and against any and all claims, demands, liabilities, losses, costs, damages, actions and causes of action by whomsoever made, sustained, brought or prosecuted in any manner based upon, occasioned by or attributable to anything done or omitted to be done by the Company, its directors, officers, employees, agents, authorized assigns or sub-contractors of the Company including negligent acts or negligent omissions in connection with duties set out above and performed, purportedly performed or required to be performed by the Company under this Agreement and including any breach of its obligations contained herein.

5. SURVIVAL. All representations, covenants, warranties, indemnities and limitations of liability set out in this agreement shall survive the termination or expiry of this agreement.

IN WITNESS WHEREOF the parties hereto have caused this Agreement to be signed by their duly authorized officers as of the date first below written.

On Behalf of
[insert name]

date

signature

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. Despite having security practices in place, information may still be vulnerable to unauthorized access due to the constantly evolving online threat landscape and/or internal threat, whether deliberate or negligent.

The following protocol outlines the Board's legal and ethical responsibility 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. The scope includes any suspected or real privacy breach that involves the Board's data or information systems.

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 types of privacy breaches:

- Unauthorized Collection – over collection of information not necessary to our purpose of providing educational support to students;
- Unauthorized access – data left unsecured or accessible to those not needing the information;
- Unauthorized Use – accessing information for a purpose other than those related to employment responsibilities and purpose;
- Unauthorized Disclosure – sharing of information with third parties or within unauthorized applications; or
- Loss or theft of information or removeable/portable media that contains personal information.

Examples include but are not limited to: 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 identify 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 include classroom applications 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, immediately notify your supervisor and the Privacy Officer who will implement concurrently the five steps of the response protocol. The Manager of Information Technology may also be contacted for urgent security breaches. The Privacy Officer and Manager of Informtion Technology can be reached by calling the Catholic Education Centre at 519-627-6762.

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.

Appendix D

TEMPLATE LETTER: USE OF SOCIAL MEDIA IN THE CLASSROOM
(on school letterhead)
[Date]

Dear Families,

This [school year/month], I will be introducing students to an exciting form of online written communication— [SCCDSB.net Google Platform/Twitter/blogging/wikis/etc]. The purpose of this letter is to share some information about [SCCDSB.net Google Platform / Twitter / blogging / wikis/etc] and to let you know how our class will use [this/these social media platform(s)].

[SCCDSB.net is a closed environment for teacher-to-student and student to student collaboration. Despite being on the Internet, the environment is not open to everyone. Teachers select who is able to access the learning resources posted on the classroom or student drive or site.]

[Twitter/Facebook is a social media network that is increasingly being used in education as a learning tool. It is widely used by teachers around the world for educational purposes and helps learning communities, students and parents build meaningful connections. These forums are on the external Internet and are open to outside users.]

[A classroom blog is a discussion or information website where permitted users add entries (posts), which are displayed in chronological order. Students will have the opportunity to write posts on a variety of topics being covered in the classroom. These writing exercises are opportunities for students to reflect upon lessons, practice their writing and critical thinking skills, and to see their learning come alive online.]

In our class, we will be using [XXX] to share some of the exciting activities we learn. Posts will be written by students and monitored and sent by the teacher. Those who follow us—[parents, other classes, teachers, community members]—will be able to read [and comment] on our posts.

A very important aspect of using social media in the classroom is digital citizenship as it relates to responsible and safe online use. Our class has discussed this in terms of our online behaviour. As a class, we agree that all of our social media posts must:

- use student first names only
- not reveal personal information about the writer or anyone else in the class
- use appropriate language
- be kind and respectful
- only include photos/videos where signed consent is on file

If you are interested in following us on [insert URL or instructions for following, e.g. Twitter, our username is @OurClass]. We hope you will enjoy reading and responding to our posts as they occur throughout the year. We are excited to give you a virtual window into our classroom!

Sincerely,
[Teacher's Name]