POLICY: Appropriate Use of Technology Guidelines

I. Purpose of Policy

As part of its curriculum the Board provides students with a digital media learning environment comprised of information and computing technologies which may include: software, Internet access, hardware (computers, printers, scanners, digital cameras, etc.).

Board staff use information and computing technologies for teaching and administrative functions which support the Board's educational mandate.

This Policy sets out standards for appropriate use of information and computing technology for educational purposes and while at school, on school-sponsored activities and/or board activities and functions. These standards apply to both board and personally-owned equipment

User acknowledgement and agreement of the appropriate use guidelines is required.

By accessing the Internet while on board property or by logging in with a board login, students and staff accept all terms and conditions of the board network and Internet use, as well as the terms outlined in this Policy.

Digital Citizenship

Digital citizenship is defined as the norms of responsible behaviour related to the appropriate use of technology. These norms and responsibilities are an expectation in all Renfrew County Catholic District School Board locations and should be clearly outlined in each school's Code of Conduct.

As individuals, we live and work in a world where people are connected to their devices at all times so we need to use technology effectively and respectfully. Digital citizenship is an important part of what the Board helps students learn in school.

Students will see teachers incorporate digital resources into their lessons. Educational online resources will be able to be accessed wirelessly through the Board's networks. As such, students will be encouraged to ***BYOD—Bring Your Own Device***. When relevant to curriculum and instruction, teachers will permit the use of any personal electronic device as a classroom learning device.

Secondary students will also be able to access educational resources using their personal devices outside the classroom, in libraries, cafeterias and other common areas.

By accessing the Internet while on RCCDSB property or by logging in with a board login, students accept all terms and conditions of the RCCDSB network and Internet use, as well as the terms outlined in this policy.

II. Policy Statement

1. Scope of Policy:

This Policy applies to all Board technology and to all personally owned technology, as defined in this Policy. The application of this Policy includes:

- the use of all Board-owned technology, such as computers, phones and mobile devices, networks, learning management systems, applications, and websites regardless of where they are used. This includes the use of Board-owned technology when used off Board property.

- the use of personally owned technology, including personally owned computers and mobile devices, when used on Board property, on the Board network or when used to access Board resources. The policy also applies to use of personally owned technology when off board property. Inappropriate use of personally owned technology, while on or off school property, that has a negative impact on school climate will result in a full investigation and necessary action will be taken, where appropriate. Consequences for inappropriate use are outlined both in the Code of Conduct as well in the Board's Safe Schools policy.
- any access to Board technology resources regardless of the location and ownership of the device used to access Board resources. Specifically, the Policy applies to home, remote, or wireless access to the Board network, websites and applications.
- the use of third-party information technology services provided to the Board. This includes Internet services provided by the Ministry of Education.

2. Five Guiding Principles:

A. Intended use:
Board technology is provided for educational and administrative purposes. Technology should be used for these intended purposes only.

B. Security and safety of Board data:
Users should take reasonable precautions to ensure that the data that they use is secure and safe. Data should be used for the intended purposes only.

C. Responsible resource usage:
The Board's technology resources are shared and limited. Users should use technology resources responsibly and should not waste resources. Personal materials should not be stored on Board property.

D. Legal compliance:
Users are expected to comply with federal and provincial legislation, as well as Board Policies.

E. Ownership of data:
Board technology and all data stored on Board technology are owned and may be accessed by the Board. Users should have no expectation of privacy in anything they create, store, send or receive using Board technology.

3. Appendices from Guiding Principles:

All users are responsible for compliance with the Appendices derived from the Guiding Principles.

4. Responsibilities:

a) All users are responsible for:

- ensuring that technology is used in accordance with Board policies and procedures,
- complying with the school's Code of Conduct,
- ensuring that technology is used to support teaching and learning in accordance with the Board's teaching and learning expectations,
- using technology in a lawful, responsible and ethical manner consistent with the purposes for which it is provided,
- their personal network login and password—it should not be shared with anyone other than a parent/guardian (students),
- ensuring that photos, videos or images of an individual/group are not posted online/shared digitally unless consent from the individual(s)—over the age of 18—or parental consent (for those under the age of 18) has been obtained.
- technology is not used for political or union business unless approved by the board.

b) Superintendents, principals and managers/supervisors are responsible for:
- ensuring that staff are aware of the Board policy,
- establishing and monitoring appropriate use through the school's Code of Conduct,
- instructing and modeling, appropriate use for staff and students.

c) Teachers are responsible for:
- the supervision of student use of technology within the teacher's assigned teaching area,
- instructing and modeling, for students, digital citizenship and responsibility,
- determining when students are able to access Board technology or their personally owned devices.

d) Students are responsible for:
- using Board technology for curriculum-related/educational purposes only,
- using personally owned technology for curriculum-related/educational purposes and behaving as an appropriate digital citizen,
- demonstrating appropriate use of technology, as outlined in schools' codes of conduct,
- reporting any inappropriate use of email, social media, data or unauthorized technology to a teacher or administrator immediately,
- the care, maintenance and security of their personal devices—the Board is not responsible for the replacement of lost, stolen or damaged items.

5. Consequences (Remedial and Disciplinary Action)

Individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the school Code of Conduct, progressive discipline and Safe Schools legislation. Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:
- limitations being placed on access privileges to personal and Board technology resources,
- suspension of access privileges to personal and Board technology resources,
- revocation of access privileges to personal and Board technology resources,
- appropriate disciplinary measures (staff), up to and including dismissal,
- appropriate progressive discipline measures (students) within Bill 212 (Progressive Discipline and School Safety),
- legal action and prosecution by the relevant authorities.

III. Definitions

Technology – Technology resources include, but are not limited to, computers, phones, cellular/mobile technology, wearable technology, servers, networks, Internet services, computer applications, data, email and collaboration tools, social media sites as well as third-party Internet services provided to the Board. Examples of third-party web services include E-Learning Ontario and online textbook providers.

User – A user is any individual granted authorization to access technology, as defined above. Users may include students, parents, staff, volunteers, visitors, contractors, or individuals employed by service providers

IV. Related Information

Appendices for this Policy

APPENDIX A: Intended Use
APPENDIX B: Security and Safety of Board Data
APPENDIX C: Responsible Resource Usage

APPENDIX D: Legal Compliance
APPENDIX E: Privacy Expectations

Related Board Policies & Information

POLICY: Commercial Electronic Messages Requirements
PROCEDURE A: Electronic Communications – Parents and Students
PROCEDURE B: Electronic Communications – Board Business
APPENDIX A: CASL – New Email Requirements
APPENDIX B: CASL – Board Business Emails

POLICY: Information (Personal) – Collection, Use and Disclosure
PROCEDURE A: Student Information
PROCEDURE B: Security Measures
APPENDIX A: Explanation Related to Student Information

Federal Legislation

Canada's Anti Spam Legislation (CASL)
Electronic Commerce Protection Regulations 2013-36
Electronic Commerce Protection Regulation 2013-221

Provincial Legislation

Education Act
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
MFIPPA, Regulation 823 (General)

Ministry of Education

Ontario Student Record (OSR) Guideline 2000

APPENDIX A: Intended Use

Intended Use
Technology is provided for educational and administrative purposes and should be used for these intended purposes only.

Prohibited Uses
Prohibited uses of technology include, but are not limited to:

- personal use that is not limited and/or occasional,
- use that violates federal or provincial laws,
- use of Board technology for commercial or political party purposes,
- use that contravenes Board Policies,
- theft of resources, including electronic data theft,
- unauthorized access, alteration, destruction, removal and/or disclosure of data. This includes the unauthorized disclosure of Board email addresses, distribution lists, and user account information.
- unauthorized access or disclosure of confidential information creating, displaying, storing or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials,
- cyberbullying,
- copying, downloading, transferring, renaming, adding or deleting information protected under copyright law,
- use that could reasonably be expected to impair the Board's computing facilities or interfere with others' use of Board technology (e.g. viruses, spam) including the sending of electronic "chain" mail,
- agreeing to license or download material for which a fee is charged to the Board without obtaining express written permission from the Board's IT staff.

Procurement
Purchasing of materials and services must comply with all procurement policies and procedures.

APPENDIX B: Security & Safety of Board Data

Users should take reasonable precautions to ensure that data that they use is secure and safe. Staff are given access to data in order to perform their job functions. Data should be used for the purposes intended. Other uses of data are strictly prohibited.

Data may include but is not limited to student records, employee records, confidential assessments, and other personal information. Data may be held in more than one format such as an electronic document (e.g. Word Document) or in a system such as email or the Student Information System. All Board data is included in this Policy.

Users are responsible for managing the accounts and passwords that provide access to data. Users are responsible for applying passwords to any personal device that accesses or holds Board data. Users will not attempt to gain unauthorized access to Board technology or data nor will they attempt to disrupt or destroy data.

Users must exercise reasonable care to ensure the safety of the data entrusted to them. All confidential data not held on Board-owned servers must be in a secured and Board authorized server. This applies to all confidential data stored on Board and personally owned computers. And Board and third party servers.

Users must comply with any security measures implemented by the Board. All files downloaded from the Internet must be scanned with Board-approved virus detection software—disabling virus scanning is strictly prohibited. Users are responsible for implementing virus scanning on personally owned devices that hold or access Board technology.

Remote or wireless access to Board resources is only permitted through the Board's approved infrastructure. Users will not attempt to by-pass the Board's security.

APPENDIX C: Responsible Resource Use

The Board's technology resources are shared and limited. Users should use technology resources responsibly and should not waste resources. As such, the Board reserves the right to limit any activity that consumes a high level of resources that may impact Board services or other users. Examples of shared resources include file storage, network bandwidth, and Internet access.

Access to Internet websites and services that significantly impact the Board Internet or network performance will be controlled. Users are not permitted to circumvent the Internet and network controls put in place.

Personal materials not relevant to educational and administrative purposes will not be stored on Board servers at any time, for any reason.

With respect to information stored for the intended purposes, the Board may impose retention periods for various information classes, either temporarily or permanently. A user should not download, copy or store files that exceed the user's data storage limit; users that do so will experience data loss.

APPENDIX D: Legal Compliance

Users are expected to comply with all federal and provincial laws and regulations including but not limited to the Education Act, the Municipal Freedom of Information and Protection of Privacy Act, the Criminal Code, Canada's Anti Spam Legislation, the Copyright Act.

The storage of unlawful materials on Board property is strictly prohibited.

Board resources may not be used in any manner to create, store, send, display or make available to others material that contravenes federal or provincial laws or regulations.

Users shall comply with all applicable Board Policies including the following:

- Commercial Electronic Messages Policy (Administration Category); and
- Information (Personal) – Collection, Use and Disclosure Policy (Administration Category).

APPENDIX E: Privacy Expectations

Board technology resources and all data stored on Board technology are owned and may be accessed by the Board. Data stored on Board technology, including email, electronic files, and information in computer systems, is Board property and may be reviewed, monitored and accessed by authorized individuals, as needed. Data is also subject to relevant legislation and may be accessed through Freedom of Information requests.

Users should not expect privacy with respect to any of their activities when using the Board's computer and/or telecommunication property, systems or services. Use of passwords or account numbers by users does not create a reasonable expectation of privacy and confidentiality of information being maintained or transmitted. The Board reserves the right to review, retrieve, read and disclose any files, messages or communications that are created, sent, received or stored on the Board's computer systems and/or equipment. The Board's right to review, also called monitoring, is for the purpose of ensuring the security and protection of business records, preventing unlawful and/or inappropriate conduct, and creating and maintaining a productive work environment. If policy violations are discovered, this will result in an investigation and necessary action will be taken, where appropriate.

Information stored on personally owned devices is the responsibility of the device owner/user. However, personally owned devices which are used for creating, displaying, storing or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials that impact school climate will result in a full investigation and necessary action will be taken, where appropriate.

POLICY: Commercial Electronic Message Requirements

I. Purpose of Policy

Canada's Anti-Spam Legislation (CASL) prohibits persons (including school boards and their employees) from sending a Commercial Electronic Message (CEM) unless:

- the recipient of the CEM has given consent,
- the CEM contains the required contact information; and
- there is a simple unsubscribe mechanism. (s. 6 (1) (2)).

This Policy provides a general outline of the requirements of Canada's Anti-Spam Legislation (CASL).

To ensure compliance with CASL Procedure A shall be used for any communications to parents and students and Procedure B shall be used for any Board business communications.

II. Policy Statement

1. Electronic Message Communications to Parents & Students

All Board employees, trustees and other persons authorized to use the Board's technology system to communicate with parents, guardians, students (18 years of age or older) and students (16 years of age or older who have withdrawn from parental control) ***shall follow Procedure A***.

2. Electronic Message Communications for Board Business

All Board employees, trustees and other persons authorized to use the Board's technology system (including all computers, databases, networks, software, email system, internet) for electronic message communications for the purpose of Board business ***shall follow Procedure B***.

3. Mandatory Contact Information & Unsubscribe Mechanism

All Board, School and related Commercial Electronic Messages (CEM's) shall contain the contact information and the unsubscribe mechanism required by the legislation.

4. Consent for Commercial Electronic Messages (CEM's)

a) Express Consent:

Board employees and trustees shall ensure that the recipient of a CEM has given his, her or its express consent to receive a CEM.

b) Implied Consent:

On occasion Supervisory Officers, Managers and employees in Plant Services and Purchasing may send a CEM to a recipient in situations where the recipient is deemed to have given his, her or its implied consent for the CEM. In situations involving implied consent the Board employee shall endeavour to obtain express consent for the CEM as soon as possible.

c) Legislative Exemption for Consent:

On occasion Supervisory Officers, Managers and employees in Plant Services and Purchasing may send a CEM to a recipient in situations where a legislative exemption for consent applies. If possible in these situations the Board employee shall endeavour to obtain express consent for the CEM as soon as possible.

5. Recording Individuals' Express Consent and Unsubscribe Requests

a) Recording Individuals' Express Consent:

The Board shall establish a system for recording all express consents to receive electronic message communications (including emails).

b) Recording Individuals' Unsubscribe Requests:

The Board shall establish a system for implementing and recording all requests to unsubscribe from electronic message communications (including emails).

6. Board Electronic Message System must not to be used for Personal Communications

a) Board Electronic Message System for Board, School and Related Matters:

Persons with access to the Board's technology system (including all computers, databases, networks, software, email system, internet) shall ensure that they do not use the system of Board electronic message communications including Board emails and Board email addresses for their personal communications.

b) Personal Employee Communications:

Board employees and trustees shall use their own personal electronic email addresses for their personal communications (e.g. Gmail, Hotmail, etc.)

7. Activities Prohibited by Canada's Anti-Spam Legislation (CASL)

Persons with access to the Board's technology system (including all computers, databases, networks, software, email system, internet) shall not use the system for any activities prohibited by CASL including without limitation the following:

a) send a Commercial Electronic Messages without the consent of the recipient and without the contact and unsubscribe information (s. 6 (1));

b) alter the transmission data in an electronic message without consent or authorization (s. 7 (1));
c) transmit, distribute or deliver any electronic message with false or misleading representations;
d) install software programs on Board, school or a person's computer system without authorization (s. 8 (1));
e) collect or use a person's electronic address through a computer program designed for collecting electronic addresses; and
f) interfere with a person's computer system without consent or authorization (s. 8).

8. Possible Maximum Penalties for Violations of Canada's Anti-Spam Legislation

The Maximum Penalty for a violation of Canada's Anti-Spam Legislation is:

- one million dollars ($1,000,000) in the case of an individual, and
- ten million dollars ($10,000,000) in the case of any other person (i.e. a corporation, etc.). (s. 20 (4))

III. Definitions

A ***person*** means an individual, partnership, corporation, organization, association, trustee, administrator, executor, liquidator of a succession, receiver or legal representative. (s. 1 (1))

Commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, (an expectation of profit is not required) other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada. (s. 1 (1))

An ***electronic address*** means an address used in connection with the transmission of an electronic message to

a) an electronic mail account;
b) an instant messaging account;
c) a telephone account; or
d) any similar account. (s. 1 (1))

An ***electronic message*** means a message sent by any means of telecommunication, including a text, sound, voice or image message. (s. 1 (1))

A ***Commercial Electronic Message*** (CEM) is an electronic message that, having regard to its content, hyperlinks, or contact information it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including an electronic message that

a) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;

b) offers to provide a business, investment or gaming opportunity;
c) advertises or promotes anything referred to in paragraph (a) or (b); or
d) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (a) to (c), or who intends to do so. (s. 1 (2))

An electronic message that contains a request for consent to send a message described above is also considered to be a commercial electronic message. (s. 1 (3))

A request for ***express consent*** must:

a) identify the purpose or purposes for which the consent is being sought;
b) include the required contact information for the sender of the CEM; and
c) include the required unsubscribe mechanism. (s. 10 (1))

The required ***contact information*** in a Commercial Electronic Message (CEM) must:

a) identify the person who sent the message and the person — if different — on whose behalf it is sent as follows:
    i) sender's personal name and their business name, if different from their personal name;
    ii) if CEM sent on behalf of another person, that person's personal name and their business name, if different from their personal name;
    iii) if CEM sent on behalf of another person, a statement indicating which person is sending the CEM and which person on whose behalf the CEM is sent;
    iv) the mailing address, and either a telephone number providing access to an agent or a voice messaging system, an email address or a web address of the person sending the message or, if different, the person on whose behalf the message is sent;
    (If it is not practicable to include the above information and the unsubscribe mechanism in the CEM, that information may be posted on a web page with a link to the web page in the CEM.)
b) and, the above information must enable the person to whom the message is sent to readily contact one of the persons referred to in paragraph (a). (s. 6 (2); Regulation 2012-36, s. 2)
    [Contact information must remain valid for a minimum of 60 days after the CEM has been sent. (s. 6 (3))]

The required ***unsubscribe mechanism*** in a Commercial Electronic Message (CEM) must:

a) enable the recipient of a CEM to indicate, at no cost, their wish to no longer receive any commercial electronic messages from the sender of the CEM, using
    i) the same electronic means by which the message was sent, or
    ii) if using those means is not practicable, any other electronic means to indicate the wish; and
b) specify an electronic address, or link to a page on the World Wide Web that can be accessed through a web browser, to which the indication may be sent. (s. 11 (1))

IV. Related Information

PROCEDURE A: Commercial Electronic Communications to Parents and Students
PROCEDURE B: Commercial Electronic Communications for Board Business

Related Board Policies

POLICY: Appropriate Use of Technology Guidelines
APPENDIX A: Intended Use
APPENDIX B: Security and Safety of Board Data
APPENDIX C: Responsible Resource Usage
APPENDIX D: Legal Compliance
APPENDIX E: Privacy Expectations

Federal Legislation

Canada's Anti-Spam Legislation (CASL)
Electronic Commerce Protection Regulations 2013-36
Electronic Commerce Protection Regulation 2013-221

PROCEDURE A: Electronic Message Communications to Parents & Students

I. Overview / Procedure Description

Canada's Anti-Spam Legislation (CASL) prohibits persons (including school board personnel) from sending a Commercial Electronic Message (CEM) unless:

- the recipient of the CEM has given consent,
- the CEM contains the required contact information; and
- there is a simple unsubscribe mechanism. (CASL, s. 6 (1) (2))

II. Areas of Responsibility

All Board employees, trustees and other persons authorized to use the Board's technology system (including all computers, databases, networks, software, email system, internet) to communicate with parents, guardians and students ***shall follow this Procedure*** to ensure that any electronic message communications to parents, guardians and students comply with the Canada's Anti-Spam Legislation (CASL).

III. Procedure Steps / Checklist

1. What is an Electronic Message

An electronic message includes a message (text, sound, voice or image) sent by means of telecommunications to:

- an electronic mail account (email),
- an instant messaging account (Facebook Messenger, Twitter, WhatsApp, other messaging apps);
- a telephone account (texts) or
- any similar account. (CASL, s. 1 (1))

2. What is a Commercial Electronic Message (CEM)

If one of the purposes of an electronic message is to encourage participation in a commercial activity (purchasing, selling, providing a business opportunity, or advertising of such an activity), the message is a commercial electronic message. (CASL, s. 1 (1))

3. Social Media Posting by Schools

Canada's Anti-Spam Legislation does not apply to the passive posting of content on social media (Facebook, Twitter, LinkedIn, blog, etc.). This type of social media posting is not considered a direct electronic delivery to an electronic address (email, instant message, telephone or other similar account).

4. General Electronic Messages to Parents, Guardians & Students

a) Parent Group Email List:
Board employees, trustees and other persons authorized to use the Board's technology system to communicate with parents, guardians, students (18 years of age or older) and students (16 years of age or older who have withdrawn from parental control) ***shall use the Parent Group Email List*** for any such electronic message communications.

b) Express Consents are Recorded in the Parent Group Email List
A group email list of all parents, guardians, students (18 years of age or older) and students (16 years of age or older who have withdrawn from parental control), who have given express consent to receive Board electronic message communications, has been created on the Board's general Microsoft Office platform (***the Parent Group Email List).***

c) Mandatory Contact and Unsubscribe Information in the Parent Group Email List:
Emails sent from the Parent Group Email List have the contact information and unsubscribe mechanism required by Canada's Anti-Spam Legislation (CASL).

d) Unsubscribe Requests are Handled by the Parent Group Email List
A request to unsubscribe from a recipient of an email sent from the Parent Group Email List will remove the recipient's name and electronic email address from the Parent Group Email List.

5. Superintendent Approval Required for Electronic Messages to Parents, Guardians & Students Using any Other Electronic Messaging Apps

Superintendent approval is required before any Board employees, trustees and other persons authorized to use the Board's technology system communicate with parents, guardians, students (18 years of age or older) and students (16 years of age or older who have withdrawn from parental control) using ***any other electronic messaging app***.

IV. Related Information

Procedures and Appendices for this Policy

POLICY: Commercial Electronic Message Requirements
PROCEDURE B: Commercial Electronic Communications – Board Business

Federal Legislation

Canada's Anti-Spam Legislation (CASL)
Electronic Commerce Protection Regulations 2013-36
Electronic Commerce Protection Regulation 2013-221

PROCEDURE B: Electronic Message Communications for Board Business

I. Overview / Procedure Description

Canada's Anti-Spam Legislation (CASL) prohibits persons (including school boards) from sending a Commercial Electronic Message (CEM) unless:

- the recipient of the CEM has given consent,
- the CEM contains the required contact information; and
- there is a simple unsubscribe mechanism (CASL, s. 6 (1) (2))

unless a statutory exemption applies.

II. Areas of Responsibility

All Board employees, trustees and other persons authorized to use the Board's technology system (including all computers, databases, networks, software, email system, internet) to communicate for Board business purposes ***shall follow this Procedure*** to ensure that any electronic message communications for the purpose of Board business comply with the Canada's Anti-Spam Legislation (CASL).

III. Procedure Steps / Checklist

1. What is an Electronic Message

An electronic message includes a message (text, sound, voice or image) sent by means of telecommunications to:

- an electronic mail account (email),
- an instant messaging account (Facebook Messenger, Twitter, WhatsApp, other messaging apps);
- a telephone account (texts) or
- any similar account. (CASL, s. 1 (1))

2. What is a Commercial Electronic Message (CEM)

If one of the purposes of an electronic message is to encourage participation in a commercial activity (purchasing, selling, providing a business opportunity, or advertising of such an activity), the message is a commercial electronic message. (CASL, s. 1 (1))

3. General Electronic Messages for Board Business Purposes

a) Board Business Group Email
Board employees, trustees and other persons authorized to use the Board's technology system to communicate with persons for the purpose of Board business shall use the ***Business Group Email List*** for any such electronic message communications unless a legislative exemption is applicable or Superintendent approval has been given for another electronic messaging app.

b) Express Consents are Recorded in the Business Group Email List
A group email list of all business individuals or entities who have given express consent to receive Board electronic message communications has been created on the Board's general Microsoft Office platform ***(the Business Group Email List);***

c) Mandatory Contact and Unsubscribe Information in the Business Group Email List:
Emails sent from the Business Group Email List have the contact information and unsubscribe mechanism required by Canada's Anti-Spam Legislation (CASL).

d) Unsubscribe Requests are Handled by the Business Group Email List
A request to unsubscribe from a recipient of an email sent from the Business Group Email List will remove the recipient's name and electronic email address from the Business Group Email List.

4. CEM Exceptions to Consent, Contact Information & Unsubscribe Mechanism Requirements:

The following Commercial Electronic Messages (CEM's) are exempt from the consent, contact information and unsubscribe requirement of CASL:

a) A CEM that is sent by or on behalf of an individual to another individual with whom they have a **personal or family relationship** as defined by the Regulations.
b) A CEM that is sent to a person who is engaged in a **commercial activity** and consists solely of an inquiry or application related to that activity. (s. 6 (5))
c) A CEM that is of a class or is sent in circumstances listed below:
    i) CEM's between employees, representatives and consultants within an organization where the CEM concerns the organization's activities **[internal Board communications];**
    ii) CEM's between employees, representatives and consultants of one organization with employees, representative and consultants of another organization where organizations have a relationship and the CEM concerns the activities of the organization to which the CEM is sent **[external Board communications]**;

iii) A CEM that is sent in **response** to a request, inquiry or complaint or is otherwise solicited by the person to whom the message is sent.

iv) A CEM that is sent to a person: to satisfy a **legal** or juridical obligation; to provide notice of an existing or pending **right**, to enforce a legal or juridical **obligation**, court order, judgment or tariff; to **enforce** a right, legal or juridical obligation, court order, judgment or tariff, or; to enforce a right arising under a **law** of Canada, of a province or municipality of Canada or of a foreign state.

5. CEM Exceptions to Consent Requirements Only (Contact Information and Unsubscribe Mechanism Required):

Consent is not required for a CEM that:

a) provides a quote or estimate for the supply of a product, goods, a service, land or an interest or right in land requested by the recipient of the CEM;

b) facilitates, completes or confirms a previously agreed commercial transaction between the sender and recipient of the CEM;

c) provides warranty information, product recall information or safety or security information about goods or services purchased or used by the recipient of the CEM:

d) provides notification of factual information about the ongoing use or ongoing purchase by the recipient of a CEM of a product, goods or a service offered under a subscription, membership, account, loan or similar relationship; or about the said ongoing subscription, membership, account, loan or similar relationship:

e) provides information directly related to an employment relationship or related benefit plan in which the recipient of the CEM is currently involved, participating or enrolled;

f) delivers an agreed product, goods or a service, including product updates or upgrades the recipient is entitled to receive;

g) communicates for a purpose specified in the regulations (the first CEM after a referral from a person with an existing business, family or personal relationship). (s. 6 (6))

6. Implied Consent Situations:

Consent is implied if:

a) the sender of the CEM has an existing business relationship with the person to whom it is sent;

b) the recipient of the CEM has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address and the message is relevant to the person's business, role, functions or duties in a business or official capacity;

c) the recipient of the CEM person has disclosed, to the sender of the CEM, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity.

7. Obtaining Express Consent in Implied Consent Situations:

In situations where the recipient of the CEM is deemed to have given his, her or its implied consent, the Board employee should always endeavour to obtain express consent as soon as possible.

8. Record of CEM sent with Implied Consent

A record of all CEM's sent where the recipient was deemed to have given implied consent shall be maintained along with the supporting documentation for the implied consent.

9. Superintendent Approval Required for Electronic Messages for Board Business Purposes Using any Other Electronic Messaging Apps

Superintendent approval is required before any Board employees, trustees and other persons authorized to use the Board's technology system communicate for Board business purposes using ***any other electronic messaging app***.

IV. Definitions

A ***person*** means an individual, partnership, corporation, organization, association, trustee, administrator, executor, liquidator of a succession, receiver or legal representative. (s. 1 (1))

Commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, (an expectation of profit is not required) other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada. (s. 1 (1))

An ***electronic address*** means an address used in connection with the transmission of an electronic message to

a) an electronic mail account;
b) an instant messaging account;
c) a telephone account; or
d) any similar account. (s. 1 (1))

An ***electronic message*** means a message sent by any means of telecommunication, including a text, sound, voice or image message. (s. 1 (1))

A ***Commercial Electronic Message (CEM)*** is an electronic message that, having regard to its content, hyperlinks, or contact information it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including an electronic message that

a) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
b) offers to provide a business, investment or gaming opportunity;
c) advertises or promotes anything referred to in paragraph (a) or (b); or
d) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (a) to (c), or who intends to do so. (s. 1 (2))

An electronic message that contains a request for consent to send a message described above is also considered to be a commercial electronic message. (s. 1 (3))

A request for ***express consent*** must:

a) identify the purpose or purposes for which the consent is being sought;
b) include the required contact information for the sender of the CEM; and
c) include the required unsubscribe mechanism. (s. 10 (1))

The required ***contact information*** in a Commercial Electronic Message (CEM) must:

a) identify the person who sent the message and the person — if different — on whose behalf it is sent as follows:
    i) sender's personal name and their business name, if different from their personal name;
    ii) if CEM sent on behalf of another person, that person's personal name and their business name, if different from their personal name;
    iii) if CEM sent on behalf of another person, a statement indicating which person is sending the CEM and which person on whose behalf the CEM is sent;
    iv) the mailing address, and either a telephone number providing access to an agent or a voice messaging system, an email address or a web address of the person sending the message or, if different, the person on whose behalf the message is sent;
    (If it is not practicable to include the above information and the unsubscribe mechanism in the CEM, that information may be posted on a web page with a link to the web page in the CEM.)

b) and, the above information must enabling the person to whom the message is sent to readily contact one of the persons referred to in paragraph (a). (s. 6 (2); Regulation 2012-36, s. 2)
[Contact information must remain valid for a minimum of 60 days after the CEM has been sent. (s. 6 (3))]

The required ***unsubscribe mechanism*** in a Commercial Electronic Message (CEM) must:

a) enable the recipient of a CEM to indicate, at no cost, their wish to no longer receive any commercial electronic messages from the sender of the CEM, using
   i) the same electronic means by which the message was sent, or
   ii) if using those means is not practicable, any other electronic means to indicate the wish; and
b) specify an electronic address, or link to a page on the World Wide Web that can be accessed through a web browser, to which the indication may be sent. (s. 11 (1))

An ***existing business relationship*** means a business relationship between sender and recipient of CEM arising from:

a) the purchase or lease of a product, goods, a service, land or an interest or right in land, by the recipient of the CEM from the sender of the CEM within the two-year period immediately before the day on which the message was sent;
b) the acceptance by the recipient of the CEM within the two year period in subsection (a) of a business, investment or gaming opportunity offered by the sender of the CEM;
c) the bartering of anything mentioned in paragraph (a) between the sender and the recipient of the CEM within the two year period in subsection (a);
d) a written contract entered into between the sender and the recipient of the CEM in respect of a matter not referred to in any of paragraphs (a) to (c), if the contract is currently in existence or expired within the two year period in subsection (a); or
e) an inquiry or application, within the six month period immediately before the day on which the message was sent, made by the recipient of the CEM to the sender of the CEM in respect of anything in (a) to (c). (s. 10 (10))

V. Related Information

Procedures and Appendices for this Policy

POLICY: Commercial Electronic Message Requirements
PROCEDURE A: Commercial Electronic Communications to Parents and Students

Federal Legislation

Canada's Anti-Spam Legislation (CASL)
Electronic Commerce Protection Regulations 2013-36
Electronic Commerce Protection Regulation 2013-221

POLICY: Complaint

I. Purpose of Policy

The Complaint Process ensures that any individual's concern will be given respectful attention while upholding the integrity of the educational system. It provides clear procedures for the communication and resolution of any concern held by members of our Educational Community including parents, students, Board employees and members of the public.

II. Policy Statement

1. Scope of Policy:

a) Subject Matter of a Complaint:

You may make a complaint about any decision or recommendation made or any act done or omitted in the course of the administration of the Renfrew County Catholic District School Board which affects you in your personal capacity save and except for matters set out in Section 2 of this Policy.

b) Other Complaint Processes:

If your complaint concerns a matter which is covered in another complaint process, statutory process or legal process, including matters in Section 2; you must use the other process.

c) Timelines for Complaints:

There is an expectation that formal written complaints shall be filed within six (6) months of the decision or action which is the subject matter of the complaint, unless the delay was justified because of extenuating circumstances and would not result in substantial prejudice to anyone.

2. Matters covered in Other Complaint Processes:

a) Identification, Placement and Review of Exceptional Students:

Matters dealing with the identification, placement and review of exceptional students shall be dealt through the Board's Identification, Placement and Review Committees (IPRC) and related bodies mandated by section 57 of the Education Act, Ontario Regulation 306 (Special Education Programs and Services) and Ontario Regulation181/98 (Identification and Placement of Exceptional Pupils) and any related Ministry of Education Directives.

b) Pupil Bullying, Discipline, Suspension and Expulsion:

Matters related to pupil bullying, discipline, suspension, expulsion and related matters shall be dealt with under the Board's Safe Schools Policies and Procedures, the applicable sections of the Education Act and its Regulations, and related Ministry of Education Directives. The Board's Safe Schools Policies are in the Schools & Students Policy Category on the Board website (Our Board / Policies and Procedures / Schools & Students).

c) Student Transportation Issues:

The Renfrew County Joint Transportation Consortium (RCJTC) is a non-for-profit organization set up between the Renfrew County Catholic District School Board and the Renfrew County District School Board to provide safe, cost effective, on time delivery of transportation services for the students in Renfrew County. The RCJTC oversees all home to school bus scheduling for the Renfrew County Catholic District School Board and the Renfrew County District School Board.

Where a parent/guardian or adult student disagrees with the way in which policies and procedures have been applied by the RCJTC, the parent/guardian or adult student may appeal the decision using the *Procedure AP.04.07: Process for Appealing Decisions*. Procedure AP.04.07 is set out on the RCJTC website (About Us / Policies and Procedures / Procedures / Operational Procedures).

d) Collective Agreement Disputes:

All differences between the Board, a union and employees arising from the interpretation, application, administration or alleged violation of the agreement, including any question as to whether a matter is arbitrable shall be dealt with under the Grievance and Arbitration provisions of the applicable collective agreement.

e) Human Rights Complaints:

Complaints related to discrimination, harassment and/or failure to accommodate shall be dealt with under the Board's Human Rights Policy and related Procedures. These Policies and Procedures are on the Board website (Our Board / Policies and Procedures / Human Resources).

At his or her option the complainant may file a formal complaint with the Ontario Human Rights Tribunal. A unionized employee complainant may file a grievance under the Grievance and Arbitration Procedure in his or her collective agreement.

f) Workplace Violence and Harassment Complaints and Reports:

Complaints or reports of workplace violence and/or harassment shall be dealt with under the Board's Workplace Violence Policy and Workplace Harassment Policy and their related Procedures in the Human Resources Policy Category on the Board website (Our Board / Policies and Procedures / Human Resources).

3. Informal Resolution Process:

a) Board Employee Administrative Decision, Action or Non Action:

STEP 1: Where possible the complaint should discuss the matter with the Board employee responsible for the administrative decision, action or non action.

STEP 2: If the complainant is dissatisfied with Step 1 or for some reason the complainant cannot talk to the Board employee responsible for the administrative decision, action or non action; the complainant should discuss the matter with the relevant supervisory officer (Superintendent of Educational Services or Superintendent of Business Services).

b) Director of Education Decision, Action or Non Action:

Where possible the complainant should discuss the matter with the Director of Education.

c) Board of Trustees Decision, Action or Non Action:

Where possible the complainant should discuss the matter with the Chair or the Vice-Chair of the Board of Trustees.

4. Formal Written Complaint:

If the complaint has not been resolved by the informal resolution process, the complainant may file a written complaint using the Form set out in Appendix A – Formal Complaint Form.

5. Board Discretion not to Deal with a Complaint:

The Board, in its discretion, may refuse to deal with a complaint:

a) if the complainant had knowledge of the decision, action or non action for six months before the filing of the complaint;
b) if the subject matter of the complaint is trivial;
c) if the complaint is frivolous or vexatious; or
d) if the complainant does not have a sufficient personal interest in the subject matter of the complaint.

If the Board refuses to deal with your complaint, it will advise you in writing together with its reasons for the refusal.

6. Board Response to a Formal Written Complaint:

The Board Response to a formal written complaint shall follow the guidelines set out in Procedure A – Response to Complaint.

7. Communication of the Results of the Review:

The Board will advise you in writing of the results of its review and of any action it is proposing to take or has taken.

III. Related Information

Procedures for this Policy

PROCEDURE A: Response to Complaint
APPENDIX A: Formal Complaint Form

PROCEDURE A: Response to Complaint

I. Overview / Procedure Description

The Board shall follow these guidelines in the review of and response to formal written complaints.

I. Procedure Steps / Checklist

1. General Process:

a) The Board will notify the Board employee and tell him about the decision, action or non action which is the subject matter of your complaint.
b) If your complaint concerns the elected Board of Trustees, the Board will notify the Chair or the Vice-Chair of the Board and tell him about the decision, action or non action which is the subject matter of your complaint.
c) The employee, the Chair or the Vice-Chair of the Board shall have an opportunity to respond to your complaint in writing.
d) The Board may share this response with you.
e) Both you and the employee, the Chair or the Vice Chair of the Board may be asked for further information.
f) The process shall be carried out within a reasonable time frame.

2. Review of the Decision, Action or Non Action:

a) Board Employee Administrative Decision, Action or Non Action:
A Supervisory Officer (Superintendent of Educational Services or Superintendent of Business Services) who is not the subject matter of the complaint and who has not been involved in the informal resolution process shall review the subject matter of the complaint, the written complaint, the written response to the complaint and any additional information.

b) Director of Education Decision, Action or Non Action:
A Supervisory Officer (Superintendent of Educational Services or Superintendent of Business Services) who is not the subject matter of the complaint and who has not been involved in the informal resolution process shall review the subject matter of the complaint, the written complaint, the written response to the complaint and any additional information.

c) Board of Trustees Decision, Action or Non Action:
The Chair, the Vice Chair or a Trustee designated by the Board who is not the subject matter of the complaint and who has not been involved in the informal resolution process shall review the subject matter of the complaint, the written complaint, the written response to the complaint and any additional information.

3. Results of Review:

The results of the review of your complaint may include:

a) dismissing your complaint;
b) taking what action appears necessary;
c) recommending to the Director of Education to take what action appears necessary; or
d) recommending to the elected Board of Trustees to take what action appears necessary.

4. Record:

The Board shall maintain a record of the original written complaint, the written response, any additional information, the results of the review and any resulting action.

APPENDIX A: Formal Complaint Form

First Name:	Address:
Last Name:	
Phone:	
Alt. Phone:	City / Province
Email:	Postal Code:
Best Contact Method:	

1. Please provide the name of the School and location, if applicable.

2. How would you describe your relationship or role with the School or the School Board.

3. If you are a parent or guardian, please provide the name of the student involved and his or her school.

4. Please describe the matter you are complaining about.

5. What steps have you taken to resolve your complaint. (Please include any names and titles of persons you have dealt with as well as relevant dates.

6. Please describe and attach any relevant documents.

I have read the Board Complaint Policy and Procedure A – Response to Complaint. I wish you to deal with my complaint under the above Policy and Procedure.

Signature Date

EMAIL: jperry@rccdsb.edu.on.ca

MAIL: Mr. Jaimie Perry, Director of Education,
Renfrew County Catholic District School Board,
499 Pembroke Street West, Pembroke, ON K8A 5P1

POLICY: Cyber-Protection

I. Purpose of Policy

The Board Cyber-Protection Plan is designed to manage cyber risks and mitigate current and evolving cyber threats to:

- Personal information and other board confidential information,
- Board information systems, network and devices,
- Education technology applications and tools,
- Internet connected equipment used in the management of board facilities,
- Staff, students and others when online and using board-provided technology.

II. Policy Statement

1. Board's Cyber-Protection Plan

The Board shall design, implement and test a Cyber-Protection Plan.

2. Appendix A – Cyber Incident Response Plan Checklist

Board staff shall design, implement and test a Cyber Incident Response Plan using the Appendix A Checklist.

3. Appendix B – Immediate Action for Serious Cyber Incidents

A serious cyber incident requires immediate action. A checklist has been set out in Appendix B.

4. Appendix C – Declared (Serious) Cyber Incident Reports

The Ministry of Education has set out the timelines and required reports for a Declared Cyber Incident (i.e., a serious cyber incident).

5. Appendix D – Other Cyber Incident Reports

The Ministry of Education has set out the required reports for Other Cyber Incidents (non-declared, safety and security tool generated).

III. Definitions

A ***cyber incident*** is an unauthorized cyber security event, or a series of such events, that has the potential to compromise an organization's business operations including:

- accidental data losses, such as an employee misplacing a USB,
- criminal attacks,
- issue motivated groups and
- state sponsored actors.

A ***declared cyber incident*** presents a significant probability of compromising the availability, integrity, or confidentiality of board systems and/or data.

Examples can include:

- a widespread phishing or ransomware attack,
- compromise of admin level credentials,
- major breach of personal or sensitive information,
- denial of service to multiple board external systems.

A ***non-declared cyber incident*** is simple in nature and can be handled by the board utilizing their standard IT incident management process. These incidents do not have any data loss, and do not represent a significant probability of compromising business operations.

Examples include:

- include single student account compromise,
- small number of malware infected computers,
- Port scans of external board systems,
- lost/stolen laptop/mobile device (that is encrypted and does not contain sensitive data).

A cyber safety incident has an online student safety component. These incidents are generally online manifestations of safety and student well-being concerns that are typically handled through the board's safe school process and where board IT may play a supporting role.

Examples include:

- cyber bullying,
- sextortion,
- cyber predators,
- safety related phishing attacks on the students,
- scams directed at students.

A ***security tool generated cyber incident*** may be automatically identified, and cyber incident records generated in a security tool, if a board is using advanced cyber security incident detect and response capabilities (e.g., SIEM/SOAR and/or EDR/XDR).

These automatically generated incidents can include early indicators of anomalous activity or deviation from pre-established policies in the board's IT environment that usually require timely action to avoid escalating into a full-fledge declared incident.

A ***Cyber-Protection Plan*** is a written document that contains behavioral and technical guidelines for all employees to ensure maximum protection from cybersecurity incidents and ransomware attacks.

Ransomware is a type of malware that denies a user's access to a system or data until a sum of money is paid.

IV. Related Information

Procedures and Appendices for this Policy

APPENDIX A: Cyber Incident Response Plan Checklist
APPENDIX B: Immediate Action for Serious Cyber Incidents
APPENDIX C: Declared (Serious) Cyber Incident Reports
APPENDIX D: Other Cyber Incident Reports

Related Policies, Procedures and Appendices (Human Resources Policy Category)

Information (Confidential) - Collection, Use & Disclosure
Technology – Responsible Use

Related Policies, Procedures and Appendices (Schools & Students Policy Category)

Digital Citizenship
Information (Student) - Collection, Use & Disclosure

Legislation

Criminal Code (cyber crimes ss. 342.1 & 342.2)
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Government Reports

Canadian Centre for Cyber Security. (30-Nov-2021). *Ransomware Play Book*. Ottawa: Government of Canada, Communications Security Establishment

Ministry of Education. (1-Feb-2023). *K-12 Cyber Protection Framework and Standards – Cyber Incident Response Standard.* Government of Ontario.

APPENDIX A: Cyber Incident Response Plan Checklist

Priority	***Action / Responsibility***	***Requirements***
1.	*Risk Assessment* *(Technology & Security Services Department)*	☐ Identify key systems and assets critical to Board business operations. ☐ Analyze the likelihood and impact of these systems being compromised. ☐ Prioritize response efforts to ensure the most critical systems and assets are protected and backed up offline frequently and securely.
2.	*Policy Documents* *(Consultant / Superintendent)*	☐ Develop an incident response policy that establishes the authorities, roles, and responsibilities for your organization (Consultant). ☐ Ensure pre-authorizations to contract assistance are established and communicated to key incident response contacts (Superintendent).
3.	*Cyber Incident Response Team (CIRT)* *(Superintendent / Technology & Security Services Department)*	☐ Create a CIRT to assess, document, and respond to incidents, restore your systems, recover information, and reduce the risk of the incident reoccurring. ☐ Include employees with various qualifications and have cross-functional support from other business lines. ☐ Designate backup responders to act for any absent CIRT members in the event of an incident.
4.	*Training* *(Superintendents / Technology & Security Services Department)*	☐ Tailor your training programs to the Board's operational needs and requirements, as well as its roles and responsibilities. ☐ Ensure your training includes standard cyber security controls including malicious emails and phishing attacks and strong passwords. ☐ Consult the Cyber Centre Learning Hub for advice and guidance on cyber security event management training. The Learning Hub offers a comprehensive event management course that can be tailored to an organization's operational and IT needs.
5.	*Identify Stakeholders* *(Superintendents)*	☐ Identify the internal and external key stakeholders who will be notified during an incident including: ○ third parties and managed service providers, ○ law enforcement and/or the Board lawyer, ○ others.

6.	*Communications* *(Superintendents)*	☐ Detail how, when, and with whom your team communicates. ☐ Include a central point of contact for employees to report suspected or known incidents. ☐ Ensure you have external contact information for all members and backup members of your response team, key personnel, and key stakeholders. ☐ Prepare sample media statements that can be tailored to cyber incidents as they occur. ☐ Consider retaining a third party organization who can guide you through your incident response and recovery process.
7.	*Auditing & Updating* *(Superintendents & Technology & Security Services Department)*	☐ Specify reason for Plan update if not part of annual update. ☐ Annual Plan update for beginning of School Year (1-Sep). ☐ Determine type of biannual Plan audit (Internal, External, MOE). ☐ Biannual audit of Plan for 30-Jun. ☐ Detailed Update / Audit Report to Director, Supervisory Officers, Manager of Technology and Security Services. ☐ Necessary changes to the Cyber Protection Plan documents.

Canadian Centre for Cyber Security. (30-Nov-2021). *Ransomware Play Book*. Ottawa: Government of Canada, Communications Security Establishment (pp. 14-15)

Ministry of Education. (1-Feb-2023). *K-12 Cyber Protection Framework and Standards – Cyber Incident Response Standard.* Government of Ontario.

APPENDIX B: Immediate Action for Serious Cyber Incidents

Priority	***Action / Responsibility***	***Detailed Steps***
1.	*Determine what is infected and isolate.* *(Superintendents & Technology & Security Services Department)*	☐ Determine which devices and systems are infected with the ransomware / malware. ☐ Isolate all infected systems and devices. ☐ Disconnect the infected systems and devices from any network connection to reduce the risk of the infection spreading to other connected devices. You may also need to disconnect them from the Internet. ☐ Determine what data, even in-transit data, has been impacted by the ransomware / malware. ☐ Establish the likelihood of the confidentiality or integrity of the data being compromised and inform data managers and stakeholders of potential impacts. ☐ Possibly disable your virtual private networks, remote access servers, single sign on resources, and cloud-based or public-facing assets as additional measures to contain the ransomware infection.
2.	*Report to Law Enforcement & Others* *(Superintendents & Technology & Security Services Department)*	☐ Report the cyber attack to OPP (1-888-310-1122). Ransomware is considered a cybercrime and may be investigated by law enforcement. ☐ Law enforcement may be able to provide you with a decryption key if you have been infected with a known type of ransomware. ☐ Ministry of Education and Cyber Security Ontario. ☐ Report the cyber attack to the Canadian Anti-Fraud Centre and the Cyber Centre online via My Cyber Portal.
3.	*Report any Privacy Breach to the Ontario Information & Privacy Commissioner* *(Superintendents)*	☐ Consult the relevant Information (Student) Collection, Use & Disclosure Policy document for a student privacy breach (Schools & Students Policy Category). ☐ Consult the relevant Information (Confidential) Policy document for a staff or other privacy breach (Human Resources Policy Category). ☐ Make the necessary reports.

Appendix B: Immediate Action for Serious Cyber Incidents

4.	*Report to OSBIE* *(Superintendent of Business Services)*	☐ Report serious cyber incidents to the Board's Insurer OSBIE. ☐ Advise OSBIE of the: o impact on Board systems and technology, o Board response, o time to remediate.
5.	*Report to Board* *(Superintendent)*	☐ Report serious cyber incidents to the elected Board of Trustees in Committee of the Whole Board (closed session). ☐ Advise the elected Board of Trustees in Committee of the Whole Board (closed session) of the: o impact on Board systems and technology, o Board response, o time to remediate. ☐ Provide periodic updates as required.
6.	*Assemble Cyber Incident Response Team (CIRT)* *(Superintendents & Technology & Security Services Department)*	☐ Communicate the incident details to your CIRT. ☐ Provide clear direction to CIRT members on their roles and responsibilities in managing the incident. ☐ Document the known details to ensure your CIRT has an initial understanding of what has occurred. ☐ Triage the systems impacted by the ransomware malware for restoration and recovery. This will assist your CIRT with where to focus immediate actions.
7.	*Change Credentials* *(Security Services Department)*	☐ Reset credentials, like passwords and passphrases, for administrator and user accounts. ☐ Ensure you are not changing any credentials that are required to restore your backup or may lock you out of systems needed during the recovery process. ☐ Create temporary administrator accounts to begin your recovery and monitor whether your original accounts are being leveraged by the threat actor.
8.	*Wipe and Reinstall* *(Security Services Department)*	☐ Safely wipe your infected devices to remove any malware, bugs, or viruses. ☐ Reinstall the operating system to rid your devices of the infection.
9.	*Run Security Software* *(Security Services Department)*	☐ Run anti-virus and anti-malware diagnostics on your backup to make sure it is clean before you begin the restore process. ☐ Scan any files that might have been accessed by the threat actor or extracted from a compromised system. See the Cyber Centre's website to download their free malware detection and analysis tool Assemblyline. ☐ Address any items flagged by the scans.

10.	*Other Reporting* *(Superintendents & Technology & Security Services Department)*	☐ Consult Appendix C – Declared Cyber Incident for timelines and other reporting. ☐ Make the necessary reports.

Canadian Centre for Cyber Security. (30-Nov-2021). *Ransomware Play Book*. Ottawa: Government of Canada, Communications Security Establishment (pp. 26-27 as modified for an Ontario District School Board)

Ministry of Education. (1-Feb-2023). *K-12 Cyber Protection Framework and Standards – Cyber Incident Response Standard.* Government of Ontario.

APPENDIX C: Declared (Serious) Cyber Incident Reports

A ***declared cyber incident*** presents a significant probability of compromising the availability, integrity, or confidentiality of board systems and/or data.

Examples can include a widespread phishing or ransomware attack, compromise of admin level credentials, major breach of personal or sensitive information, denial of service to multiple board external systems.

Timeline	*Action*	*Cyber Incident Information*
Initial Report (0-4 hrs.)	*Report to OPP (1-888-310-1122), MOE, Cyber Security Ontario, 3rd Party Security Providers, Canadian Anti-Fraud Centre, and the Cyber Centre online via My Cyber Portal.* *If privacy breach, report to Ontario Information & Privacy Commissioner.* *If third party vendors involved, report to them.*	☐ Incident type: ○ Ransomware, ○ Widespread Phishing Attack, ○ Board Confidential information Data Breach, ○ Personal Information Data Breach, ○ Multiple End User Impact, ○ Administration Level Credential Impact, ○ Major Denial of Service to Board External Systems, ○ Other: _____ ☐ Incident Time / Date: _____ ☐ Systems Impacted: _____ _____ _____ ☐ Personal Information Privacy Breach: _____ _____ ☐ Student Safety Impacted: _____ _____ ☐ Time to Contain: _____ ☐ Time to Remediate: _____ ☐ Other Relevant Information: _____ _____ _____

Full Report (24-48 hrs.)	*Full Report to same Parties as Initial Report.*	☐ Initial Report Information. ☐ Root Cause Analysis. ☐ Issues and Risks. ☐ Timelines for Follow Up Action.
Response Notices (72-96 hrs.)	*Response Notices to same Parties as Initial Report.*	☐ Incident Summary Information. ☐ Root Cause Analysis Summary. ☐ Plan to remediate. ☐ Remediation Timeline ☐ Issues and Risks.
Update Notices (every 8-24 hours during remedia-tion)	*Update Notices to same Parties as Initial Report.*	☐ Remediation Tasks completed. ☐ Remediation Tasks in progress. ☐ Completion Timeline. ☐ Next Update Timeline.
Incident Closed Notice (within 24 hours of completion)	*Incident Closed Notices to same Parties as Initial Report.*	☐ Tasks done to contain breach. ☐ Root Cause Analysis. ☐ Tasks completed. ☐ Remaining Issues and Risks. ☐ Long Term Tasks Outstanding.
Lessons Learned (within 2 weeks of completion)	*Lessons Learned Information to same Parties as Initial Report.*	☐ Identified issues, risks and vulnerabilities not directly related to the cyber incident. ☐ Task required for remediation. ☐ Timeline for remediation.

Ministry of Education. (1-Feb-2023). *K-12 Cyber Protection Framework and Standards – Cyber Incident Response Standard.* Government of Ontario.

APPENDIX D: Other Cyber Incident Reports

A ***non-declared cyber incident*** is simple in nature and can be handled by the Board utilizing their standard IT incident management process. These incidents do not have any data loss, and do not represent a significant probability of compromising business operations.

Examples include:

- include single student account compromise,
- small number of malware infected computers,
- Port scans of external board systems,
- lost/stolen laptop/mobile device (that is encrypted and does not contain sensitive data).

A cyber safety incident has an online student safety component. These incidents are generally online manifestations of safety and student well-being concerns that are typically handled through the Board's safe school process and where Board IT may play a supporting role.

Examples include:

- cyber bullying,
- sextortion,
- cyber predators,
- safety related phishing attacks on the students,
- scams directed at students.

A ***security tool generated cyber incident*** may be automatically identified, and cyber incident records generated in a security tool, if a board is using advanced cyber security incident detect and response capabilities (e.g., SIEM/SOAR and/or EDR/XDR).

These automatically generated incidents can include early indicators of anomalous activity or deviation from pre-established policies in the board's IT environment that usually require timely action to avoid escalating into a full-fledge declared incident.

Appendix D: Other Cyber Incident Reports

Cyber Incident	*Element*	*Cyber Incident Information / Action*
Non-Declared	*Incident Occurs*	☐ Cyber Incident Threat: o Ransomware Attempt, o Phishing Attack, o Board Confidential information Data Attack, o Personal Information Data Attack, o Single End User Impact, o Some Malware infected computers, o Minor Denial of Service to Board External Systems, o Other: _____ ☐ Incident Time / Date: _____ ☐ Other Relevant Information: _____
	Response	☐ Determine any risks to Board systems and technology. ☐ Take any necessary precautions.
	Reporting	☐ Report quarterly to MOE (Incident Dates & Threat Types).
Safety	*Incident Occurs*	☐ Cyber Incident: o cyber bullying, o sextortion, o cyber predators, o safety related phishing attacks on the students, o scams directed at students. o Other: _____ ☐ Incident Time / Date: _____ ☐ Other Relevant Information: _____
	Response	☐ Determine risks to Board systems and technology. ☐ Take any necessary precautions.
	Reporting	☐ Report quarterly to MOE (Incident Dates & Threat Types).

Appendix D: Other Cyber Incident Reports

Security Generated	*Incident Occurs*	☐ Cyber Incident Threat: _____ _____ _____ ☐ Incident Time / Date: _____ ☐ Other Relevant Information: _____ _____ _____
	Response	☐ Determine risks to Board systems and technology. ☐ Take any necessary precautions.
	Reporting	☐ Report quarterly to MOE (Incident Dates & Threat Types)

Ministry of Education. (1-Feb-2023). *K-12 Cyber Protection Framework and Standards – Cyber Incident Response Standard.* Government of Ontario.

POLICY: Human Rights

I. Purpose of Policy

The Ontario Human Rights Code:

- recognizes the dignity and worth of every person and
- provides every person with equal rights and opportunities without discrimination in the area of services and employment.

As part of an inclusive Catholic educational community and in accordance with the Board's Vision Statement Board employees and trustees strive to:

- foster a world view shaped by the Catholic conversation about life's meaning and purpose;
- nurture the giftedness, self-worth and potential of each individual;
- reverence the dignity of the whole person.

This Policy sets out the commitment of Renfrew County Catholic District School Board to respect and abide by the above principles.

II. Policy Statement

1. The Human Right Code:

a) Services without Discrimination (s.1):
Every person has a right to equal treatment with respect to services, goods and facilities, without discrimination because of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, gender identity, gender expression, age, marital status, family status or disability

b) Employment without discrimination (s. 5 (1)):
Every person has a right to equal treatment with respect to employment without discrimination because of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, gender identity, gender expression, age, record of offences, marital status, family status or disability.

c) Freedom from Harassment in Employment (s. 5 (2)):
Every person who is an employee has a right to freedom from harassment in the workplace by the employer or agent of the employer or by another employee because of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sexual orientation, gender identity, gender expression, age, record of offences, marital status, family status or disability.

d) Freedom from Harassment because of Sex in the Workplace (s. 7 (2)):
Every person who is an employee has a right to freedom from harassment in the workplace because of sex, sexual orientation, gender identity or gender expression by his or her employer or agent of the employer or by another employee.

e) Definition of Disability (s. 10 (1))):
"disability" means,

a) any degree of physical disability, infirmity, malformation or disfigurement that is caused by bodily injury, birth defect or illness and, without limiting the generality of the foregoing, includes diabetes mellitus, epilepsy, a brain injury, any degree of paralysis, amputation, lack of physical co-ordination, blindness or visual impediment, deafness or hearing impediment, muteness or speech impediment, or physical reliance on a guide dog or other animal or on a wheelchair or other remedial appliance or device,
b) a condition of mental impairment or a developmental disability,
c) a learning disability, or a dysfunction in one or more of the processes involved in understanding or using symbols or spoken language,
d) a mental disorder, or
e) an injury or disability for which benefits were claimed or received under the insurance plan established under the Workplace Safety and Insurance Act, 1997; ("handicap")

2. The Board is committed to:

- ensuring a healthy and inclusive environment for its employees, students and its broader educational community;
- preventing and addressing discrimination and harassment; and
- if a person requires accommodation on one of the enumerated grounds in the Human Rights Code, providing such accommodation in accordance with the Code.

3. Accommodation:

The principle of accommodation applies to all grounds of the Code, but accommodation issues in employment most often relate to the needs of:

- employees with disabilities (disability);
- older workers (age);
- employees with religious needs (creed);
- pregnant women (sex); and
- employees with caregiving responsibilities (family status).

[Ontario Human Rights Commission. *Human Rights at Work 2008 – Third Edition*, p. 93)

III. Complaint Process and Accommodation Process Checklist

1. Complaint Process:

The components of the Board's Human Rights Complaint Process are set out in Procedure A to this Policy.

2. Accommodation Process Checklist:

Appendix A sets out the obligations of employees, the employees' supervisors (including Principals / Vice-Principals), and the Board administration in any human rights accommodation situation.

IV. Definitions

Discrimination Components:

- a distinction or differential treatment based on grounds related to the personal characteristic of the individual or group;
- a distinction or differential treatment related to one or more grounds of discrimination in the Human Rights Code; and
- the distinction creates a disadvantage or limits opportunity for the individual.

The duty to accommodate is an obligation to meet the special needs of persons protected by the Human Rights Code unless meeting such needs would create undue hardship.

Harassment means engaging in a course of vexatious comment or conduct, which is related to one of the grounds in the Human Rights Code, against a worker in a workplace that is known or ought reasonably to be known to be unwelcome.

V. Related Information

Procedures for this Policy

PROCEDURE A: Complaint Process
APPENDIX A: Accommodation Process Checklist

Related Policies

POLICY: Attendance Support
POLICY: Workplace Violence
POLICY: Workplace Harassment

Legislation

Human Rights Code

PROCEDURE A: Human Rights Complaint Process

I. Overview / Procedure Description

This Procedure outlines the requirements for reporting, investigating and responding to human rights complaints.

II. Procedure Steps / Checklist

1. Written Complaint to the Manager of Human Resources Services:

a) Human rights complaints shall be made promptly, in writing, and no more than one year from the date of the incident or one year from the last incident in a series of related incidents.

b) The written complaint shall:

- provide the complainant's contact information (name, home address or work location, phone/cell and email);
- describe the particulars of the incident(s) or situation (date, time, location and what happened);
- identify the relevant persons involved (name, contact information, status (employee, student, other));
- set out any other relevant information;
- furnish the remedy sought; and
- list the applicable section of the Human Rights Code.

c) The written complaint shall be given to the Manager of Human Resources Services who shall give a copy of the complaint to the relevant Superintendent.

2. Confidentiality:

As much as possible confidentiality will be maintained in the process. However, the right of an alleged offender to know the case against him or her, reporting obligations, the obligation to investigate and the obligation to take any necessary action means that absolute confidentiality cannot be guaranteed to the employee filing the complaint or report.

3. Representation for an Alleged Offender / Complainant

a) An alleged offender who is a unionized employee has a right to have his or her union representative present at any investigative meeting or a meeting which may result in disciplinary action. An alleged offender who is not a unionized employee has a right to have a representative present at any investigative meeting or a meeting which may result in disciplinary action.

b) A complainant who is a unionized employee has a right to have his or her union representative present at any meeting resulting from an incident or complaint. A complainant who is not a unionized employee has a right to have a representative present at any meeting resulting from an incident or complaint.

4. Interim Action:

After a written complaint of discrimination and/or harassment has been received, the Manager of Human Resources Services shall assess whether any interim action is required to provide the complainant with a environment free from discrimination and/or harassment.

5. Informal Resolution:

In less serious incidents an informal resolution process may be used to attempt to resolve the dispute between the parties to the alleged incident(s) or situation.

6. Investigation

Written human rights complaints shall be investigated promptly. Prior to making a final decision on the complaint the alleged offender shall be given the particulars of the complaint / investigation and provided with an opportunity to make a written response to the allegations.

7. Assessment of the Complaint:

The response of the alleged offender shall be considered prior to making a determination of what happened and what action should be taken.

8. Reporting to the Complainant:

The complainant shall be advised of the results of the investigation and of the action the Board has taken to maintain a violence free workplace.

9. Record of Complaint, Investigation & Response:

a) The report of the investigation, supporting documents and Board response shall be retained by the Manager of Human Resources Services in a confidential Board Folder. If discipline was administered as a result of the workplace violence, the necessary disciplinary documentation shall be filed in the employee's personnel file.

b) If the complaint was resolved by an informal resolution process, a record shall be kept of the original complaint, the results of the informal dispute resolution process and the records from any follow up or monitoring of the situation.

10. Alternative Routes for Dealing with Complaints:

At any stage in, before or after this process, a complainant may choose to refer the complaint to the Police, the Human Rights Tribunal of Ontario, or their Professional Organization or Association. The Manager of Human Resources Services may choose to involve the Police.

III. Related Information

Related Policies / Procedures

POLICY: Human Rights
APPENDIX A: Accommodation Process Checklist

Appendix A: Accommodation Process Checklist

The most appropriate accommodation is one that most:

- *respects the dignity of the employee;*
- *responds to the employee's individualized needs; and*
- *maximizes the employee's integration and full participation in the workplace.*

However, the duty to accommodate does not require exempting an employee from performing the essential requirements of the employee's job.

1. Obligations of the Employee:

☐ Advise the employee's supervisor that the employee requires accommodation under the Human Rights Code to perform the essential duties of the employee's position;

☐ Make her or his needs known to the best of his or her ability, in writing;

☐ Answer questions or provide information regarding relevant restrictions or limitations, including information from health care professionals, where appropriate and as needed;

☐ Participate in discussions regarding possible accommodation solutions;

☐ If the employee is a union member, the employee's union representative will also participate in discussions regarding possible accommodation solutions and may be present for any meetings with management representatives;

☐ Co-operate with any experts whose assistance is required to manage the accommodation process or when information is required that is unavailable to the person requesting accommodation;

☐ Meet agreed-upon performance and job standards once accommodation is provided;

☐ Work with the Human Resources Supervisor and the employee's supervisor on an ongoing basis to manage the accommodation process; and

☐ Report any problems with the accommodation process, in writing, to the employee's supervisor and/or to the Human Resources Supervisor.

2. Obligations of the Employee's Supervisor and/or Principal / Vice-Principal:

☐ Be alert to the possibility that an employee may need an accommodation even if they have not made a specific or formal request;

☐ Advise the Human Resources Supervisor of the request for accommodation or the potential for an accommodation request;

☐ Assist the Human Resources Supervisor in developing accommodation solutions;

☐ Assist the Human Resources Supervisor in implementing the required workplace accommodation;

☐ Monitor the workplace accommodation and advise the Human Resources Supervisor of any problems.

3. Obligations of the Board:

☐ Accept the employee's request for accommodation in good faith, unless there are legitimate reasons for acting otherwise;

☐ Obtain expert opinion or advice where needed;

☐ Limit requests for information to those reasonably related to the nature of the limitation or restriction so as to be able to respond to the accommodation request;

☐ Take an active role in ensuring that alternative approaches and possible accommodation solutions are investigated, and canvass various forms of possible accommodation and alternative solutions, as part of the duty to accommodate;

☐ Consult with the employee and the employee's union representative (if the employee is a union member) with respect to alternative approaches and possible accommodation solutions;

☐ Communicate regularly and effectively with the employee and the employee's union representative (if the employee is a union member) with updates on the accommodation process;

☐ Grant accommodation requests in a timely manner, to the point of undue hardship, even when the request for accommodation does not use any specific formal language;

☐ Bear the cost of any required medical information or documentation;

☐ Implement accommodation in a timely way to the point of undue hardship;

☐ Keep a record of the accommodation request and action taken; and

☐ Maintain confidentiality as much as possible.

[(27-Jun-16). Ontario Human Rights Commission. *Policy on Ableism and Discrimination based on Disability,* pp. 41-42]

Appendix B: Student Accommodation Process Checklist

The most appropriate accommodation is one that most:

- *respects the dignity of the student;*
- *responds to the student's individualized needs; and*
- *maximizes the student's integration and full participation in school.*

1. Obligations of the Parent / Guardian or Adult Student (18 years & older):

☐ Advise the School Principal that the student requires accommodation under the Human Rights Code to fully access the Board's educational program;

☐ Make the student's needs known, in writing;

☐ Answer questions or provide information regarding the accommodation including information from health care professionals, where appropriate and as needed;

☐ Participate in discussions regarding possible accommodation solutions;

☐ Co-operate with any experts whose assistance is required to manage the accommodation process or when information is required that is unavailable to the student requesting accommodation;

☐ Work with the School Principal and student's teacher(s) on an ongoing basis to manage the accommodation process; and

☐ Report any problems with the accommodation process, in writing, to the School Principal and/or to the applicable Superintendent of Educational Services.

2. Obligations of the Student's Principal and Teacher(s):

☐ Be alert to the possibility that a student may need an accommodation even if they have not made a specific or formal request;

☐ Advise the School Principal / Superintendent of Educational Services of the request for accommodation or the potential for an accommodation request;

☐ Assist in developing accommodation solutions;

☐ Assist in implementing the required accommodation;

☐ Monitor the accommodation and advise the School Principal / Superintendent of Educational Services of any problems.

3. Obligations of the Board:

☐ Accept the student's request for accommodation in good faith, unless there are legitimate reasons for acting otherwise;

☐ Obtain expert opinion or advice where needed;

☐ Limit requests for information to those reasonably related to the nature of the limitation or restriction imposed by the disability so as to be able to respond to the accommodation request;

☐ Take an active role in ensuring that alternative approaches and possible accommodation solutions are investigated, and canvass various forms of possible accommodation and alternative solutions, as part of the duty to accommodate;

☐ Consult with the student's parent / guardian or with the adult student (18 years and older) with respect to alternative approaches and possible accommodation solutions;

☐ Communicate regularly and effectively with the student's parent / guardian or with the adult student (18 years and older) with updates on the accommodation process;

☐ Grant accommodation requests in a timely manner, to the point of undue hardship, even when the request for accommodation does not use any specific formal language;

☐ Implement accommodation in a timely way to the point of undue hardship;

☐ Keep a record of the accommodation request and action taken; and

☐ Maintain confidentiality as much as possible.

[Modification of the (27-Jun-16). Ontario Human Rights Commission. *Policy on Ableism and Discrimination based on Disability, (*pp. 41-42) to fit an education situation.]

POLICY: Information (Health) – Collection, Use & Disclosure

I. Purpose of Policy

The *Personal Health Information Protection Act* (PHIPA) sets out rules for the collection, use and disclosure of personal health information by health information custodians. Health information custodians employed or under contract to the Board include physiotherapists, psychologists, psychotherapists, speech and language pathologists and social workers.

This policy sets out the information practices mandated by the PHIPA which the above health information custodians are required to follow.

In addition to this Policy, health information custodians are required to follow the health information provisions of their Regulated Health Professions College.

II. Policy Statement

1. Consent for Collection, Use or Disclosure of Health Information

a) Board Consent Form:
With some limited exceptions a health information custodian must have an authorized individual sign a consent for the collection, use or disclosure of a student's health information. (The Board Consent Form for Speech Language Services is set out in Appendix A.)

b) Direct Collection of Health Information:
Generally, a student's health information will be collected directly from a student 16 years of age or older and / or the student's custodial parent(s) where the student is under the age of 16.

c) Withdrawal of Consent Not Retroactive (PHIPA, s. 19 (1)):
If an individual has consented to the collection, use or disclosure of the individual's health information by a health information custodian; the individual may withdraw the consent by providing notice to the health information custodian, but the withdrawal of the consent shall not have retroactive effect.

d) Student's Capacity to Consent (PHIPA, s. 21 (1)):
A student is capable of consenting to the collection, use or disclosure of health information if the student is able:

- to understand the information that is relevant to deciding whether to consent to the collection, use or disclosure, as the case may be; and

- to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing the consent.

e) Parental Consent for a Student under 16 years (PHIPA, s. 23):
The custodial parent of a student, a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent may give consent for the collection, use or disclosure of the student's health information unless the information relates to:

- treatment within the meaning of the *Health Care Consent Act, 1996*, about which the student has made a decision on his or her own in accordance with that Act, or
- counselling in which the student has participated on his or her own under the *Child, Youth and Family Services Act*, *2017.*

f) Conflict between Capable Student and Custodial Parent (PHIPA, s. 23 (3):
The wishes of a student who is less than 16 years of age and who is capable of consenting to the collection, use or disclosure of the student's personal health information prevails over a conflicting decision of a custodial parent.

TABLE A: General Scheme of Authorized Consent to Student's Health Information

Age of Student	***Medical Treatment Information***	***Counselling Information***	***Health Information***
Student (under 11)	Custodial Parent(s)	Custodial Parent(s)	Custodial Parent(s)
Student (12-15) with capacity	Student's decision first, otherwise custodial parent(s)	Student's decision first, otherwise custodial parent(s)	Custodial Parent(s)
Student (16 & over) with capacity	Student	Student	Student

2. Ontario Health Cards and Health Numbers

a) Persons who provide provincially funded health resources may require individuals to produce their health cards.

b) Students or their parents may voluntarily provide Board employees with their own or their child's health card number to facilitate access to emergency health services, but Board employees cannot require the production.

c) Health card numbers which are disclosed to Board employees for the purpose of facilitating access to emergency health services shall not be used or disclosed for any other purposes.

3. Access to & Correction of Health Information Records

a) Governing Legislation:
In accordance with section 51 (3) of the *Personal Health Information Protection Act* (PHIPA) access to and correction of health information records held by health information custodians who are employees of the Board or who are acting for the Board is governed by the *Municipal Freedom of Information and Protection of Privacy Act* and in particular section 36 of that Act.

b) Applicable Board Policy:
The applicable Board Policy is the Information (Personal) - Collection, Use & Disclosure Policy.

4. Use or Disclosure of Health Information Records without Consent

If a health information custodian uses or discloses personal health information about an individual, without the individual's consent, in a manner that is outside the scope of the custodian's description of its information practices the custodian shall,

a) inform the individual of the uses and disclosures at the first reasonable opportunity unless, the individual does not have a right of access to a record of the information;
b) make a note of the uses and disclosures; and
c) keep the note as part of the records of personal health information about the individual that it has in its custody or under its control or in a form that is linked to those records. (PHIPA, s. 16)

5. Security of Health Information Records (PHIPA, s. 12)

a) Health information custodians must take steps that are reasonable in the circumstances to ensure that personal health information in their custody or control is protected from theft, loss and unauthorized use or disclosure. Records of personal health information must also be protected against unauthorized copying, modification or disposal.
b) The health information custodian must notify the applicable individuals, his or her Regulated Health Professions College and the Information and Privacy Commissioner if personal health information is stolen, lost or accessed by an unauthorized person.
c) Health information custodians shall comply with the Health Information Security Measures set out In Procedure A to this Policy.

6. Retention and Disposition of Health Information Records

a) Unless otherwise required by law, individual student health information records shall be retained for a minimum of 10 years from the last contact, or until the student turns 31.

b) After the above time the individual student health information records shall be disposed of in a secure manner unless the said record is the subject of a request for access where the request for access procedures have not been exhausted.

7. Concerns or Complaints about a Student's Health Information Record

An authorized person who has a complaint or a concern about a student's health information record shall:

a) first contact the relevant health information custodian and attempt to resolve the concern or complaint;
b) if the concern or complaint is not resolved, contact the School Board's Superintendent of Special Education (613-735-1031);
c) if the concern or complaint is not resolved, contact the Information and Privacy Commissioner of Ontario, 2 Bloor Street East, Suite 1400 Toronto, ON M4W 1A8.

III. Definitions

health care means any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that,

a) is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition,
b) is carried out or provided to prevent disease or injury or to promote health, …

In general, ***health care practitioners*** are persons involved in delivering health care who are members of a Regulated Health Professions College, which includes physiotherapists, psychologists, psychotherapists, speech and language pathologists and social workers.

health information custodians are health care practitioners who have custody or control of an individual's personal health information.

information practices, in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,

a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

personal health information means identifying information about an individual in oral or recorded form, if the information,

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is the individual's health number.

treatment means anything that is done for a therapeutic, preventive, palliative, diagnostic, cosmetic or other health-related purpose, and includes a course of treatment, plan of treatment or community treatment plan, but does not include,

- the assessment for the purpose of this Act of a person's capacity with respect to a treatment,
- the assessment or examination of a person to determine the general nature of the person's condition,
- the taking of a person's health history,
- the communication of an assessment or diagnosis,
- assistance with or supervision of hygiene, washing, dressing, grooming, eating, drinking, elimination, ambulation, positioning or any other routine activity of living (Health Care Consent Act, s. 2)

IV. Related Information

Procedure and Appendix for this Policy

PROCEDURE A: Health Information Security Measures
APPENDIX A: Consent for Speech Language Services

Related Board Policy

Information (Personal) - Collection, Use & Disclosure

Legislation

Health Care Consent Act
Municipal Freedom of Information and Protection of Privacy Act
Personal Health Information Protection Act
PHIPA, *Ontario Regulation 329/04 (General)*
Regulated Health Professions Act

Other Information

Information and Privacy Commission. (December 2004). *A Guide to the Personal Health Information Protection Act.*

PROCEDURE A: Health Information Security Measures

I. Overview / Procedure Description

One of the purposes of the Personal Health Information Protection Act (PHIPA) is to protect the privacy of individuals with respect to health information about themselves held by health information custodians employed or under contract to the School Board.

II. Areas of Responsibility

This Procedure sets out reasonable security measures and safeguards to protect the above information which health information custodians employed by or under contract to the Board must follow.

Health information custodians employed or under contract to the Board include physiotherapists, psychologists, psychotherapists, speech and language pathologists and social workers.

III. Procedure Steps / Checklist

1. Workplace Security

a) Paper and electronic files containing health information shall be kept secure at all times. For example, when transporting records, laptops, CDs, etc. care shall be taken to keep them secure.

b) All documents or files containing health information shall not be left unattended and left or in open view while in use.

c) The integrity and availability of records shall be preserved by:

i) taking records off-site only when absolutely necessary; whenever practical, the original shall remain on-site and only copies removed. OSRs shall not be removed from the school;

ii) clearly identifying copies of documents containing health information (for example IPRC packages) and destroying when no longer needed;

iii) using a sign-in/sign-out procedure including a sign out date to monitor removed files;

iv) returning records to a secure environment as quickly as possible, for example, at the end of a meeting or the end of the day.

d) All working copies of paper files containing health information shall be returned to the office or a secure environment for destruction. Records containing health or confidential information shall never be discarded in an individual's or a public trash or recycling bin.

e) Visitor access to areas where confidential information is being worked on or is stored shall be controlled. Unknown persons seen in operational areas shall be questioned e.g. Can I help you? Are you looking for someone? etc.

f) Areas of the building where health information is stored shall be secured after normal business hours.

g) Keys and access to locked file cabinets and locked areas shall be controlled and monitored.

h) When discussing a student, staff shall ensure that the conversations are professional, appropriate and respectful of the audience.

2. Computers and Electronic Information

a) Email messages shall not contain sensitive health information about an identifiable individual unless absolutely necessary. Where it is necessary to include such information in an email, consider using the individual's initials, symbols or a code rather than a full name to help maintain anonymity of the individual.

b) Computer monitors shall be positioned to minimize unauthorized viewing of the information displayed on the monitors.

c) Monitors displaying personal information shall never be left unattended and password protected screen saver options shall be used during periods of inactivity.

d) Computer hard drives and file storage media should be encrypted and must be secured against improper access by a strong password (alpha, numeric and symbol).

e) Computer hard drives and file storage media must be rendered unusable when disposed of. Contact the Helpdesk for guidance.

3. Mobile Devices

a) Mobile devices include, but are not limited to, board-owned laptops/notebook computers, integrated hand held/Personal Digital Assistants (PDAs), cellular phones removable media (flash drives, memory sticks, removable drives) that are connected to board computing devices and used to store and/or transport information to another device. Do not share or leave file storage media containing personal information unattended. Ensure that it is secured when not in use.

b) All mobile devices must be secured against improper access by a strong password (alpha, numeric and symbol). If the mobile device is used to store health or personal information, the drive must be encrypted.

c) Laptop hard drives must be encrypted and must be secured against improper access by a strong password (alpha, numeric and symbol). As much as possible health or sensitive information should not be stored on laptop hard drives. In the event that it is necessary to store data containing health information on the hard drive of a laptop, password protect the file and try to maintain the anonymity of the individual by initials or codes, etc.

d) Care must be taken when communicating health information while using a cellular or cordless telephone, as this type of communication can be easily intercepted.

4. Working from Home

Health information custodians working from home must ensure that they take reasonable steps to protect any personal information they use in their home work location by:

a) designating a secure work area as "office space" which can only be accessed by the custodian;
b) storing all work records and sensitive information in the most secure manner possible;
c) using the Board voice messaging system for conducting Board business particularly where personal information is being used;
d) avoiding saving personal work information on home computers;
e) using password protected storage media, or web enabled programs;
f) ensuring that any documents containing health information that needs to be disposed of is returned to an appropriate work location for shredding and not disposed of in the household garbage.

5. General Privacy Provisions

a) When communicating health, confidential or sensitive information, consider the physical setting and try to ensure that no one overhears the conversation, i.e. hallways, main office, etc. public telephones, etc.
b) Care must be used when transmitting health information via a fax machine. If it is necessary to fax highly sensitive health information, ensure that someone is ready to receive the transmission prior to sending it.
c) When the work environment is not conducive to privacy while collecting or communicating health information end and reschedule the conversation or move to a more private environment.

6. Privacy Breaches and Notice

A privacy breach occurs when health information is lost, stolen, or inadvertently disclosed contrary to the PHIPA. This includes the loss of computers, personal devices or media that contain personal information.

a) Notice to Ontario Information and Privacy Commissioner (PHIPA, Ontario Regulation 329/04, s. 6.3)
The health information custodian shall notify the Commissioner in the following situations if the custodian has reasonable grounds to believe that health information in the custodian's custody or control:

- was used or disclosed without authority;
- was stolen;
- is part of a pattern of similar losses or unauthorized uses or disclosures of health information; or

- the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances (sensitive, large volume or many individuals' health information, or more than one custodian involved).

b) *Annual Report to the Ontario Information and Privacy Commissioner (PHIPA, Ontario Regulation 329/04, s. 6.4)*
On or before March 1st of every year commencing in 2019 a health information custodian shall submit a report setting out the number of times in the calendar year that personal health information in the custodian's custody or control was:
- stolen.;
- lost;
- used without authority; or
- was disclosed without authority.

A copy of the above report shall be submitted to the Board's Superintendent responsible for Special Education Services.

c) *Notice to Authorized Individual (PHIPA, s. 12 (2)):*
If personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
- notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
- include in the notice a statement that the individual is entitled to make a complaint to the Commissioner.

d) *Notice to School Board Superintendent:*
If personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall, immediately notify his or her Superintendent to ensure that immediate action can be taken to mitigate the impact/results of the breach.

IV. Definitions

health care means any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that,

a) is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition,
b) is carried out or provided to prevent disease or injury or to promote health, …

In general, ***health care practitioners*** are persons involved in delivering health care who are members of a Regulated Health Professions College, which includes physiotherapists, psychologists, psychotherapists, speech and language pathologists and social workers.

health information custodians are health care practitioners who have custody or control of an individual's personal health information.

information practices, in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,

a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

personal health information means identifying information about an individual in oral or recorded form, if the information,

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is the individual's health number.

The scope of practice of a speech language pathologist is the assessment of speech and language functions and the treatment and prevention of speech and language dysfunctions or disorders to develop, maintain, rehabilitate or augment oral motor or communicative functions. (*Audiology and Speech-Language Pathology Act*, s. 3 (2))

V. Related Information

Information for this Procedure

POLICY: Information (Health) – Collection, Use & Disclosure
APPENDIX A: Consent for Speech Language Services

Legislation

Audiology and Speech-Language Pathology Act, 1991
Personal Health Information Protection Act
PHIPA, *Ontario Regulation 329/04 (General*)

Student Name	Student Date of Birth (Age)	Ontario Education No.
School (Grade)	Teacher	Male / Female

General Speech and Language Pathology Services: assessment of speech and language functions and the treatment and prevention of speech and language dysfunctions or disorders to develop, maintain, rehabilitate or augment oral motor or communicative functions.

Reason for Referral:	***Specific Services Proposed:***

Benefits of Proposed Services	***Risks / Side Effects of Proposed Services***

Alternative Options	***Consequences of Declining Proposed Services***

You may withdraw your consent to the above services at any time by notice in writing to me.

I ***consent*** to the above proposed service and I ***consent*** to the speech and language pathologist accessing my (student's) education records for the purpose of providing the proposed service.

I ***consent*** to the speech and language pathologist collecting, using and disclosing my (student's) health information for the purpose of providing the proposed service, and planning and delivering educational programs and services to meet my (student's) needs.

Print Name of Authorized Person	Signature of Authorized Person	Relationship to Student

Date Signed: _____

Student Health Information:	• the student's physical or mental health; • the student's health history and the health history of his or her family; and • any health-related observation, examination, assessment, care, service or procedure.
Purpose:	The collection, use and disclosure of a student's health information is for the purpose of planning and delivering educational programs and services to meet the student's needs.
Collection:	A student's health information will generally be collected directly from a health care practitioner, the student or his or her parent/guardian in accordance with a signed consent.
Information Storage & Retention	Health information is stored in a Student Health File and managed by the health practitioner that provided the service. Files are stored securely in a variety of formats including electronic and hard copy files. The information will be kept for a minimum of 10 years from the last contact, or until the student turns 31.
Routine Disclosure:	Unless the written consent indicates otherwise, a student's health information will be shared with the Board employees who are working directly with or who have responsibility for the student. This would normally include the school principal, vice-principal, classroom teacher, special education staff and other related staff who require this information to plan or to deliver educational programs / support for the student. Reports will be provided to the parent/guardian or student as appropriate and will be filed in the student's Ontario Student Record.
Other Permitted Disclosure	• significant risk of bodily harm of student or others (PHIPA, s. 40 (1)); • child protection (report to child and family services) (PHIPA, s. 43 (1) (e)); • legal proceeding or court / tribunal order (PHIPA, s. 41 (1)); • or otherwise permitted by law.
More Information:	Contact your school principal or review the Information (Health) - Collection, Use & Disclosure Policy.

TABLE A: General Scheme of Authorized Consent to Student's Health Information

Age of Student	***Medical Treatment Information***	***Counselling Information***	***Health Information***
Student (under 11)	Custodial Parent(s)	Custodial Parent(s)	Custodial Parent(s)
Student (12-15) with capacity	Student's decision first, otherwise custodial parent(s)	Student's decision first, otherwise custodial parent(s)	Custodial Parent(s)
Student (16 & over) with capacity	Student	Student	Student

A person is capable of consent if he or she ***understands*** the information about the proposed service and is able to ***appreciate the reasonably foreseeable consequences*** of making or not making a decision to accept the proposed service.

POLICY: Information (Personal) – Collection, Use & Disclosure

I. Purpose of Policy

The purposes of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) include protecting the privacy of individuals with respect to personal information about themselves held by institutions, including school boards, and providing individuals with a right of access to their own information. Part II (Protection of Individual Privacy) of the Act sets out restrictions on the collection, use and disclosure of personal information.

Section 265 (1) (d) of the Education Act sets out the duty of a principal to collect information for inclusion in a pupil record and section 266 of the Education Act sets out restrictions on the use and disclosure of that information.

This Policy provides guidance to Board employees, trustees, agents, independent contractors and other individuals involved with the Board as to their statutory requirements in the collection, use and disclosure of individuals' personal information including information in pupil records.

II. Policy Statement

1. Personal Information (MFIPPA) / Pupil Records (Education Act):

a) MFIPPA & Personal Information:

Personal information means recorded information about an identifiable individual, including,

i) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
ii) 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,
iii) any identifying number, symbol or other particular assigned to the individual,
iv) the address, telephone number, fingerprints or blood type of the individual,
v) the personal opinions or views of the individual except if they relate to another individual,
vi) 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,
vii) the views or opinions of another individual about the individual, and
viii) 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 (s. 2 (1)).

b) Education Act & Ontario Student Record Cards (OSR's):

A pupil record is information collected in accordance with the regulations and guidelines issued by the Minister of Education and is a record of a student's educational progress through the elementary and secondary schools of Ontario. This record is most commonly referred to as the Ontario Student Record or OSR (s. 265 (1) (d) and s. 266).

c) Personal Information / Pupil Records

A pupil record is also personal information under the MFIPPA.

2. Personal Information & Pupil Record (OSR) Information is Confidential:

a) Personal information is confidential and there are restrictions on its collection, use and disclosure in Part II of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

b) Information in a pupil record, more commonly referred to as an Ontario Student Record (OSR), is confidential and there are restrictions on its use and disclosure in section 266 of the Education Act.

3. Collection of Personal Information (MFIPPA):

a) *Collection of Personal Information:*

No person shall collect personal information on behalf of the Board unless the collection is:

i) expressly authorized by statute,
ii) used for the purposes of law enforcement or
iii) necessary to the proper administration of a lawfully authorized activity of the Board (s. 28 (2)).

b) *Direct Collection of Personal Information:*

Personal information shall be collected directly from the individual to whom the information relates unless the individual authorizes another manner of collection, another manner of collection is authorized by statute (i.e. the Education Act) or the MFIPPA authorizes another method of collection (s. 29 (1)).

c) *Notice of Collection of Personal Information:*

If personal information is collected on behalf of the Board, the Board shall inform the individual to whom the information relates of,

i) the legal authority for the collection;
ii) the principal purpose or purposes for which the personal information is intended to be used; and
iii) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection (s. 29 (2)).

4. Use of Personal Information / Pupil Records:

a) *Use of Personal Information (MFIPPA)*

The Board shall not use personal information in its custody or under its control except,

i) if the person to whom the information relates has identified that information in particular and consented to its use;
ii) for the purpose for which it was obtained or compiled or for a consistent purpose; or
iii) for a purpose for which the information may be disclosed to the Board under the MFIPPA (s. 31).

b) *Use of Pupil Records (Education Act):*

A pupil record is privileged for the information and use of supervisory officers and the principal, teachers and designated early childhood educators of the school for the improvement of instruction and other education of the pupil. (s. 266 (2)).

5. Disclosure of Personal Information / Pupil Records:

a) Disclosure of Personal Information (MFIPPA):

The Board shall not disclose personal information in its custody or under its control except,

i) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
ii) for the purpose for which it was obtained or compiled or for a consistent purpose;
iii) if the disclosure is made to an officer, employee, consultant or agent of the Board who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the Board's functions;
iv) for the purpose of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such an Act or a treaty;
v) if disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;
vi) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;
vii) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased; or
viii) as otherwise permitted under the MFIPPA (s. 32).

b) Disclosure of Pupil Records (Education Act):

i) Pupil records are not available to any other person subject to the rights of the medical officer of health, the pupil's parents or guardian where the pupil is a minor, and the pupil without the written permission of the parent or guardian of the pupil, where the pupil is a minor or of the adult pupil (s. 266 (2)).
ii) Pupil records may be disclosed to the Minister of Education and to the Board (s. 266 (7) and as otherwise required by the Act and its Regulations (s. 266 (6) (a)).
iii) However, since pupil records are personal information under the MFIPPA, these records may also be disclosed pursuant to the provisions of that Act set out in section 5 (a) above.

6. Court Action or Tribunal Proceeding:

a) A court or a tribunal has the power to compel a witness to testify or compel the production of a document which contains personal information and pupil record information (MFIPPA, s. 51 (2)).
b) In situations dealing with personal information or pupil records the witness should not disclose this information or these documents without a specific court or tribunal order.
c) A subpoena or summons to a witness is not a court or tribunal order which authorizes the release of personal information or pupil record information.

7. Proceedings under the Youth Criminal Justice Act (YCJA):

a) Priority of the YCJA over Provincial Legislation:

The YCJC is federal legislation related to criminal law and takes priority over provincial legislation.

b) Definition of Young Person:

A young person is a person between 12 and 18 years of age. (s. 2 (1))

c) Identity of Offender in YCJA Proceeding not to be Published:

Subject to the YCJA, no person shall publish the name of a young person, or any other information related to a young person, if it would identify the young person as a young person dealt with under this Act. (s. 110 (1))

d) Identity of Victim and Witness in a YCJA Proceeding not to be Published:

Subject to the YCJA, no person shall publish the name of a child or young person, or any other information related to a child or a young person, if it would identify the child or young person as having been a victim of, or as having appeared as a witness in connection with, an offence committed or alleged to have been committed by a young person. (s. 111 (1))

e) Disclosure of Record to School Personnel:

An authorized person under the YCJA may disclose to any professional or other person engaged in the supervision or care of a young person — including a representative of any school board or school— any information contained in a young person's record if the disclosure is necessary

i) to ensure compliance by the young person with an authorization related to release from a youth custody facility or an order of the youth justice court;
ii) to ensure the safety of staff, students or other persons; or
iii) to facilitate the rehabilitation of the young person.

f) Record Information to be kept Secure and Confidential:

A person to whom information from a young person's record is disclosed shall:

i) keep the information separate from any other record of the young person to whom the information relates;
ii) ensure that no other person has access to the information except if authorized under the YCJA and
iii) destroy their copy of the record when the information is no longer required for the purpose for which it was disclosed. (s. 125 (7))

8. Individual's Rights to Access and Correct his or her Personal Information / Pupil Record

a) Municipal Freedom of Information and Protection of Privacy Act (MFIPPA):

i) Every individual has a right of access to any personal information about the individual held by the Board which is reasonably retrievable by the Board (s. 36 (1)).
ii) Access to an individual's personal information held by the Board shall be in accordance with the provisions of the Act.
iii) Every individual who has been given access to his or her personal information held by the Board has a right to request correction of the personal information in accordance with section 36 (2) of the Act.

b) Education Act:

An individual's right of access to and right to request correction of a record of pupil information shall be in accordance with procedure laid out in section 266 of the Education Act.

9. Board Staff Obligations:

a) Board staff includes Board employees, trustees, agents, independent contractors and other individuals involved with the Board.

b) Board staff shall comply with legislation, Ministry directives, their own profession's standards, Board policies, procedures and agreements when collecting, using and disclosing personal information.
c) Board staff shall protect personal information by following proper procedures and best practices as outlined in Board Policies, Board Procedures and as directed by Superintendents, Managers, Principals and Supervisors.
d) Board staff shall report any suspected privacy or security breaches of which they are aware.
e) Board staff shall take reasonable steps to ensure the personal information within their custody and control is secured and protected.

10. Retention and Destruction of Personal Information / Pupil Record:

a) Personal information that has been used shall be retained for a minimum of one year (MFIPPA, Regulation 823 (General), s. 5)
b) Pupil record information shall be retained for a minimum of one year. After the one year period pupil record information shall be retained in accordance with the provisions of Section 8 of the (2000) Ontario Student Record (OSR) Guideline.
c) The Board shall establish a classification, retention and destruction schedule for all Board records.
d) Staff must ensure that records containing personal information be destroyed in a method appropriate to the medium, i.e. paper-shred, computers - rendered unusable.

III. Definitions

consistent purpose means a purpose which the individual might reasonably have expected.

law enforcement means,
a) policing,
b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
c) the conduct of proceedings referred to in clause (b)

recorded information should be viewed as being an all-inclusive term that encompasses every conceivable way that information, including data, text, image or sound, can be created, stored and retrieved electronically.

IV. Related Information

Procedures / Appendix for this Policy
PROCEDURE A: Student Information
PROCEDURE B: Security Measures
APPENDIX A: Explanation Related to Student Information

Legislation (Federal)
Youth Criminal Justice Act

Legislation (Provincial)
Education Act
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
MFIPPA, Regulation 823 (General)

Ministry of Education

Ontario Student Record (OSR) Guideline 2000.

PROCEDURE A: Information (Personal) – Student Information

I. Overview / Procedure Description

To set out guidelines for the collection, use and disclosure of student information.

II. Areas of Responsibility

All Board employees, trustees, agents, independent contractors and other individuals involved with the Board as to their statutory requirements in the collection, use and disclosure of student information.

III. Procedure Steps / Checklist

1. Information about Students & Pupil Records (OSR's) is Confidential:

a) Personal information of a student is confidential. As set out in the Board Policy (Information (Personal) – Collection, Use and Disclosure) student information is classified as personal information and there are restrictions on its collection, use and disclosure in Part II of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

b) Information in a pupil record, more commonly referred to as an Ontario Student Record (OSR), is confidential and there are restrictions on its use and disclosure in section 266 of the Education Act.

2. Direct Collection of Student Information:

a) Generally, student information is collected directly:
- from the parent or guardian of students under the age of 16;
- from the student or the parent / guardian if the student is 16 or 17 years of age;
- from the student if the student is 18 years of age or older, or
- from the student if the student is 16 or 17 years of age and has withdrawn from parental control.

b) The above individuals may authorize another manner of collection.

c) The MFIPPA may authorize another manner of collection.

CHART A: Authorized Student Information Collection

Student Information Collection	Student under 16	Student 16-17	Student 16-17 withdrawn from parental control	Student 18 & over
Authorized Person	Parent / guardian	Student or parent/guardian	Student	Student

3. Notice of Collection and Use:

a) Board forms requesting student information generally set out the following notice or its abbreviated form:

> The personal information you have provided is collected by the Renfrew County Catholic District School Board under the authority of the Education Act (R.S.O. 1990, c. E.2) ss. 58.5, 265, and 266 as amended. The information will be used to register and place the student in a school, or for a consistent purpose such as the allocation of staff and

resources. Information may be given to an insurance company if the student is involved in or witnesses an accident. The information will be used in accordance with the Education Act, the regulations, and guidelines issued by the Minister of Education governing the establishment, maintenance, use, retention, transfer, and disposal of pupil records. For questions about this collection, speak to the school principal. The contact information for your school principal can be found on the Board web site (Our Schools – School Directory).

b) An explanation of the collection and use of student information is set out in Appendix A to this Policy and is also included in student agenda documents.

4. Use of Student Information:

As set out in the above Notice student information is used for educational purposes or purposes which support educational purposes. Generally, these purposes are set out in the Education Act, its Regulations, Ministry of Education policy, memoranda and directives.

5. Disclosure of Student Information (MFIPPA):

Student information may be disclosed:

a) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
b) for the purpose for which it was obtained or compiled or for a consistent purpose;
c) if the disclosure is made to an officer, employee, consultant or agent of the Board who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the Board's functions;
d) for the purpose of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such an Act or a treaty;
e) if disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;
f) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;
g) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased; or
h) or as otherwise permitted under the MFIPPA. (s. 32)

6. Permitted Disclosures of Student Information to School Staff for Safety Reasons:

Pursuant to section 32.0.5 (3) and (4) of the Occupational Health and Safety Act the Board and Board supervisors, including Principals, have duty to provide information, including personal information, related to a risk of workplace violence from a person with a history of violent behaviour if,

i) the Board employee or service provider can be expected to encounter that person in the course of his or her work; and
ii) the risk of workplace violence is likely to expose the Board employee or service provider to physical injury.

The Board and Board supervisors shall not disclose more personal information in the circumstances than is reasonably necessary to protect a Board employee or service provider from physical injury.

7. Parent/Guardian & Student Access and Consent to Disclose Student Information:

a) Municipal Freedom of Information and Protection of Privacy Act:

i) Under the definition of personal information a pupil record is also personal information under the Act (s. 1 (2)).
ii) A child of any age has a right to access his or her personal information (s. 36 (1)).
iii) A parent who has lawful custody of a child under the age of 16 years may exercise the child's rights under the Act unless this is deemed to be an unreasonable invasion of the child's privacy. (s. 54 (c))

b) Education Act:

i) A pupil is entitled to examine his or her own pupil records (s. 266 (3)).
ii) The authority or rights of a student under the age of 18 years are vested in the parent or guardian of the student with the exception of students in subsections (iii) and (iv). (s. 1 (2))
iii) A student who is 16 or 17 years of age and who has withdrawn from parental control has the sole authority to exercise his or her rights under the Education Act.
iv) Students who are 16 and 17 years of age jointly share authority to exercise their information rights under the Education Act with their parent or guardian. The student and his or her parent or guardian each have access to the pupil record. If consent for indirect collection, non educational use or disclosure of student information is required both the student and his or her parent/guardian's must consent.
v) A student who is 18 years of age or older has the sole authority to exercise his or her rights under the Education Act.

CHART B: Parent and Student Access to Student Information

Legislation (information type)	**Student under 16**	**Student 16-17**	**Student 16-17 withdrawn from parental control**	**Student 18 & over**
MFIPPA (personal information)	Parent with lawful custody and Student	Student	Student	Student
Education Act (pupil record information–OSR)	Parent/guardian and Student	Parent/guardian and Student	Student	Student

CHART C: Parent and Student Consent to Disclose Student Information

Legislation (information type)	**Student under 16**	**Student 16-17**	**Student 16-17 withdrawn from parental control**	**Student 18 & over**
MFIPPA (personal information)	Parent with lawful custody	Student	Student	Student
Education Act (pupil record information – OSR)	Parent/guardian	Parent/guardian and Student	Student	Student

8. Custody / Access Situations and Access to Student Information:

a) Definitions:

i) Custody:
To award one parent the exclusive custody of a child is to clothe that parent, for whatever period he or she is awarded the custody, with full parental control over, and ultimate parental responsibility for, the care, upbringing and education of the child, generally to the exclusion of the right of the other parent to interfere in the decisions that are made in exercising that control or in carrying out that responsibility. (Kruger v. Kruger)

ii) Access:
The entitlement to access to a child includes the right to visit with and be visited by the child and the same rights as a parent to make inquiries and be given information as to the health, education and welfare of the child. (Ontario Children's Law Reform Act, s. 20 (5)). A spouse who is granted access to a child of the marriage in a divorce proceeding has the right to make inquiries, and to be given information, as to the health, education and welfare of the child (Divorce Act, s. 16 (5)).

iii) Joint Custody:
Joint custody is shared parental responsibility. A joint custody award gives legal custody to both parents, with care and control to one and liberal access to the other. (Baker v. Baker)

b) Legislation:

i) MFIPPA (s. 54 (c)):
For a child under the age of 16 years a custodial parent can exercise the child's rights under the Act including access to personal information under Act.

ii) Education Act (s. 1 (2)):
A parent of a child under the age of 18 years has a right to access to his or her child's pupil record.

iii) Children's Law Reform Act (s. 20 (4) and (5)):
[A right to access includes the right to access the child's education information.]
(4) Where the parents of a child live separate and apart and the child lives with one of them with the consent, implied consent or acquiescence of the other of them, the right of the other to exercise the entitlement of custody and the incidents of custody, but not the entitlement to access, is suspended until a separation agreement or order otherwise provides.
(5) The entitlement to access to a child includes the right to visit with and be visited by the child and the same right as a parent to make inquiries and to be given information as to the health, education and welfare of the child.

c) Separation Agreements and Court Orders:
Custody and access rights may be established pursuant to a signed separation agreement or pursuant to a court order.

CHART D: Separated / Divorced Parents' Access to Student Information

Family Situation with Child under 16	MFIPPA (non education personal information)	Children's Law Reform Act / Education Act (education information / pupil record)
Parents and Child living together	Either parent	Either parent
Separated Parents: Child with one parent with consent of other parent	Parent with custody of child.	Either parent
Separation Agreement: Custody to one parent and Access to the other parent	Parent with custody of child.	Either parent
Court Order: Custody to one parent and Access to the other parent	Parent with custody of child.	Either parent.
Joint Custody: Separation Agreement or Court Order	Either parent.	Either parent.

9. Student Health Card Numbers are Confidential (Personal Health Information Protection Act, s. 34)

a) Persons who provide provincially funded health resources may require individuals to produce their health cards.

b) Students or their parents may voluntarily provide Board employees with their own or their child's health card number to facilitate access to emergency health services, but Board employees cannot require the production.

c) Health card numbers which are disclosed to Board employees for the purpose of facilitating access to emergency health services shall not be used or disclosed for any other purposes.

10. Law Enforcement Disclosures:

a) Under MFIPPA disclosure of personal information is permitted to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. (s. 32 (g))

b) Law enforcement means,

i) policing,
ii) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
iii) the conduct of proceedings referred to in clause (ii). (MFIPPA, s. 2 (1))

11. Suspected Child Abuse and Disclosures to a Children's Aid Society:

a) If a person, including a person who performs professional or official duties with respect to children, has reasonable grounds to suspect child abuse, the person shall forthwith report the suspicion and the information on which it is based to a children's aid society (Child and Family Services Act, s. 72 (1)).

b) The Children's Aid Society has the right to obtain personal information from schools and school boards in order to investigate allegations or complaints around the issue of child protection. However, in such a situation, the principal or superintendent would only have been justified in disclosing information about students if a Children's Aid Society review team, or any of its members, reasonably required the information for an investigation of suspected child abuse under section 73 of the Child and Family Services Act.

12. Court / Tribunal Subpoena and Witness Obligations:

a) Consult Board Counsel:
If Board staff are served with a summons or a subpoena, they should consult Board counsel for direction and advice on their legal obligations.

b) Subpoena:
- i) Counsel for the parties to a criminal or civil trial or to an administrative hearing can require the presence of a witness to testify and to bring any requested documents, which are in his or her possession or control, by getting the court or the tribunal to issue a subpoena and serving the subpoena on the witness.
- ii) Once served with the subpoena, the witness is required to attend with the documents and remain throughout the proceedings until excused by the presiding judge.
- iii) A witness is not required to consent to being interviewed by the counsel who issued the subpoena prior to the trial or hearing.
- iv) A witness cannot release student personal information / records or staff personal information / records without an informed written consent from the individual concerned or without a specific court or tribunal order.
- v) A subpoena or a summons to a witness is not a court or tribunal order.

c) Documents containing Personal Information and/or Pupil Records:
The Education Act and the Municipal Freedom of Information and Protection of Privacy Act contain restrictions on the disclosure of student and/or staff records or information. You cannot release these document or the information contained in them without an informed written consent or an appropriate court or tribunal order unless otherwise authorized by the applicable legislation.

d) Procedure:
- i) If a witness has been subpoenaed, he or she is legally obligated to appear at the trial or hearing and to truthfully answer all the questions which he or she is asked at that time. If any documents are mentioned in the subpoena, the witness is required to bring the original of the said documents to the trial.
- ii) A subpoena is not a court or tribunal order.
- iii) Without a court/tribunal order or specific written consent you cannot discuss a student's personal information or pupil record information with counsel or disclose any documents containing a student's personal information or pupil record with counsel.
- iv) In circumstances where you are asked for personal information about a student or OSR information and no consent has been given, you should advise the court that the information is confidential pursuant to the Education Act and the Municipal Freedom of Information and Protection of Privacy Act and cannot be disclosed without a court order. You should then comply with whatever the Judge or Tribunal Chair orders.

IV. Definitions

Municipal Freedom of Information and Protection of Privacy Act / Education Act
law enforcement means,
- i) policing,
- ii) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
- iii) the conduct of proceedings referred to in clause (ii). (MFIPPA, s. 2 (1))

personal information means recorded information about an identifiable individual, including,

i) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
ii) 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,
iii) any identifying number, symbol or other particular assigned to the individual,
iv) the address, telephone number, fingerprints or blood type of the individual,
v) the personal opinions or views of the individual except if they relate to another individual,
vi) 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,
vii) the views or opinions of another individual about the individual, and
viii) 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 (MFIPPA, s. 2 (1)).

pupil record means in accordance with the Education Act, the regulations and the guidelines issued by the Minister, the information collected for inclusion in a record in respect of each pupil enrolled in the school, more commonly referred to as the Ontario Student Record (OSR) (Education Act, s. 265 (1) (d) and 266).

Occupational Health and Safety Act

employer means a person who employs one or more workers or contracts for the services of one or more workers and includes a contractor or subcontractor who performs work or supplies services and a contractor or subcontractor who undertakes with an owner, constructor, contractor or subcontractor to perform work or supply services;

worker means a person who performs work or supplies services for monetary compensation but does not include an inmate of a correctional institution or like institution or facility who participates inside the institution or facility in a work project or rehabilitation program; (s. 1 (1))

V. Related Information

Information for this Procedure

POLICY: Information (Personal) – Collection, Use & Disclosure
PROCEDURE B: Security Measures
APPENDIX A: Explanation Related to Student Information

Legislation

Children's Law Reform Act
Divorce Act
Child and Family Services Act
Education Act
Municipal Freedom of Information and Protection of Privacy Act
Occupational Health and Safety Act
Personal Health Information Protection Act

Ministry of Education

Ontario Student Record (OSR) Guideline 2000.

PROCEDURE B: Information (Personal) - Security Measures

I. Overview / Procedure Description

One of the purposes of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA) is to protect the privacy of individuals with respect to personal and health information about themselves held by institutions, including school boards.

This Procedure sets out reasonable security measures and safeguards to protect the above information.

II. Areas of Responsibility

All Board employees, trustees, agents, independent contractors and other individuals involved with the Board must follow these reasonable security measures and safeguards to protect the above information.

III. Procedure Steps / Checklist

1. Workplace Security

a) Paper and electronic files containing personal information shall be kept secure at all times. For example, when transporting records, laptops, CDs, etc. care shall be taken to keep them secure.

b) All documents or files containing personal information shall not be left unattended and left or in open view while in use.

c) The integrity and availability of records shall be preserved by:

i) taking records off-site only when absolutely necessary; whenever practical, the original shall remain on-site and only copies removed. OSRs shall not be removed from the school;

ii) clearly identifying copies of documents containing personal information (for example IPRC packages) and destroying when no longer needed;

iii) using a sign-in/sign-out procedure including a sign out date to monitor removed files;

iv) returning records to a secure environment as quickly as possible, for example, at the end of a meeting or the end of the day.

d) All working copies of paper files containing personal information shall be returned to the office or a secure environment for destruction. Records containing personal or confidential information shall never be discarded in an individual's or a public trash or recycling bin.

e) Visitor access to areas where confidential information is being worked on or is stored shall be controlled. Unknown persons seen in operational areas shall be questioned e.g. Can I help you? Are you looking for someone? etc.

f) Areas of the building where personal information is stored shall be secured after normal business hours.

g) Keys and access to locked file cabinets and locked areas shall be controlled and monitored.

h) When discussing a student, staff shall ensure that the conversations are professional, appropriate and respectful of the audience.

2. Computers and Electronic Information

a) Email messages shall not contain sensitive personal information about an identifiable individual unless absolutely necessary. Where it is necessary to include such information in an email, consider using the individual's initials, symbols or a code rather than a full name to help maintain anonymity of the individual.

b) Computer monitors shall be positioned to minimize unauthorized viewing of the information displayed on the monitors.

c) Monitors displaying personal information shall never be left unattended and password protected screen saver options shall be used during periods of inactivity.

d) Computer hard drives and file storage media should be encrypted and must be secured against improper access by a strong password (alpha, numeric and symbol).

e) Computer hard drives and file storage media must be rendered unusable when disposed of. Contact the Helpdesk for guidance.

3. Mobile Devices

a) Mobile devices include, but are not limited to, board-owned laptops/notebook computers, integrated hand held/Personal Digital Assistants (PDAs), cellular phones removable media (flash drives, memory sticks, removable drives) that are connected to board computing devices and used to store and/or transport information to another device. Do not share or leave file storage media containing personal information unattended. Ensure that it is secured when not in use.

b) All mobile devices must be secured against improper access by a strong password (alpha, numeric and symbol). If the mobile device is used to store personal information, the drive must be encrypted.

c) Laptop hard drives must be encrypted and must be secured against improper access by a strong password (alpha, numeric and symbol). As much as possible personal or sensitive information should not be stored on laptop hard drives. In the event that it is necessary to store data containing personal information on the hard drive of a laptop, password protect the file and try to maintain the anonymity of the individual by initials or codes, etc.

d) Care must be taken when communicating personal information while using a cellular or cordless telephone, as this type of communication can be easily intercepted.

4. Working from Home

Individuals working from home must ensure that they take reasonable steps to protect any personal information they use in their home work location by:

a) designating a secure work area as "office space" which can only be accessed by the individual;
b) storing all work records and sensitive information in the most secure manner possible;
c) using the Board voice messaging system for conducting Board business particularly where personal information is being used;
d) avoiding saving personal work information on home computers;
e) using password protected storage media, or web enabled programs;
f) ensuring that any documents containing personal information that needs to be disposed of is returned to an appropriate work location for shredding and not disposed of in the household garbage.

5. General Privacy Provisions

a) When communicating personal, confidential or sensitive information, consider the physical setting and try to ensure that no one overhears the conversation, i.e. hallways, main office, etc. public telephones, etc.
b) Care must be used when transmitting personal information via a fax machine. If it is necessary to fax highly sensitive personal information, ensure that someone is ready to receive the transmission prior to sending it.
c) When the work environment is not conducive to privacy while collecting or communicating personal information, end and reschedule the conversation or move to a more private environment.

6. Privacy Breaches and Notice

a) A privacy breach occurs when personal information is lost, stolen, or inadvertently disclosed contrary to the *Education Act* or the MFIPPA. This includes the loss of computers, personal devices or media that contain personal information.
b) In accordance with MFIPPA, individuals shall be informed when the security of their personal information is breached.
c) If staff becomes aware of a privacy breach, they must immediately notify their supervisor to ensure that immediate action can be taken to mitigate the impact/results of the breach. For information about responding to a privacy breach, contact your Superintendent.

IV. Related Information

Information for this Procedure

POLICY: Information (Personal) – Collection, Use & Disclosure
PROCEDURE A: Student Information
APPENDIX A: Explanation Related to Student Information

Legislation

Education Act
Municipal Freedom of Information and Protection of Privacy Act

Ministry of Education

Ontario Student Record (OSR) Guideline 2000.

APPENDIX A: Information (Personal) – Explanation Related to Student Information

Notice of routine Collection and Use of Student Personal information

The purpose of this notice is to make you aware of how the Renfrew County Catholic District School Board (Renfrew CDSB) and your school use the personal information you provide to us, in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The MFIPPA is a law that sets guidelines that schools and district school boards must follow when collecting, using and/or disclosing students' personal information. Under this Act, personal information refers to recorded information about an identifiable individual.

The Education Act sets out duties and powers of the board and authorizes school boards to collect personal information for the purpose of planning and delivering educational programs and services which best meet students' needs and for reporting to the Minister of Education, as required. In addition, the information may be used to attend to matters of health and safety or discipline which best meet student needs and for reporting to the Minister of Education, as required. The Act requires that the school principal maintain an Ontario Student Record (OSR) for each student attending the school. The OSR is a record of a student's educational progress through school in Ontario, and follows students when they transfer schools. The Ontario Student Record Guideline sets out how OSRs are to be managed and the Renfrew CDSB adheres to the OSR Guideline.

Under the MFIPPA, personal information may be used or disclosed by the Renfrew CDSB:

- for the purpose for which it was obtained or a consistent purpose (a purpose consistent with the reason collected);
- to board officers or employees who need access to the information in the performance of their duties, if necessary, and proper in the discharge of the board's authorized functions;
- to comply with legislation, a court order or subpoena or to aid in a law enforcement investigation conducted by a law enforcement agency;
- to report to the Children's Aid Society regarding child protection matters, in accordance with the law in compelling circumstances affecting health or safety of staff or students.

In accordance with MFIPPA and the Education Act, releasing personal information for any other purpose requires the informed consent of:

- the parent/guardian for children under 16 years of age;
- the parent/guardian and the student where the student is 16 and 17;
- the student where the student is over 18 or is 16 or 17 years of age and has withdrawn from parental control.

It is our practice to include a notice statement on forms used to collect personal information to advise you how we will use and disclose the information. To help you understand how we use the information you provide to us, we draw your attention to the following routine uses and/or disclosures of student personal information so that you may express any concerns you may have.

Routine uses and/or disclosures of student personal information

The student's OSR will be used by school and board staff to support the classroom teacher in developing an educational program which best meets the student's needs. Staff working with the classroom teacher or directly with the student may include individuals working in areas such as special education, guidance counselling, student success, etc.

In keeping with *21st century learning*, the Board provides students and teachers with Office 365 for Education, Google Docs for Education (GAFE) and the Ministry of Education Desire to Learn (D2L) for educational purposes. In addition, students may also use social media tools such as wikis, blogs, podcasts, video conferencing, YouTube, Facebook, Twitter and other sites or tools deemed appropriate by the classroom teacher. Students receive age-appropriate instruction on digital citizenship and the safe use of technology. Use of the Internet and social media sites shall be in accordance with the Appropriate Use Guidelines for students and posting of personal information shall be with parental consent, where appropriate.

Email addresses (parent and student) will be used for communication between home and school/board.

Contracted photographers will take individual and class photos of students. These photos will be used for administrative and archival purposes, on student cards, in school yearbooks and will be offered to parents for purchase.

Student medical health information provided by parents/ guardians or adult students will be used to address the student's medical needs at school and during school activities. Medical emergency plans for students with life-threatening medical conditions will be shared with school staff, the Renfrew County Joint Transportation Consortium, contracted bus operators and bus drivers and will be posted in identified areas of the school for emergency response purposes.

Surveillance equipment may be used in schools and on buses to enhance the safety of students and staff, to protect property against theft or vandalism and to aid in the identification of intruders or persons who endanger the health, well-being or safety of school community members.

Student personal information such as home addresses, student photos, life-threatening medical emergency information, accessibility and safety needs will be shared with the Renfrew County Joint Transportation Consortium, contracted bus company operators and bus drivers for the purpose of administering the board's contracted bus program and for the safety of students.

Birthdays may be announced over the PA system and/or in classrooms. Class lists with student first names and last initial only may be distributed to other parents for the purpose of addressing greeting cards or invitations in connection with holidays, birthday parties, etc.

Student work, including student first name and last initial may be displayed throughout the school and in school and board newsletters or websites. It may also be publicly displayed at community events such as science fairs, colouring/writing/poster contests or similar events outside the school.

Students may be recorded or photographed as part of their educational program for assessment and evaluation purposes. Photos or recordings may be shared with students and parents for the purpose of celebrating and memorializing the student's life at school.

School activities and events may be reported in school and board newsletters and on school and board websites. This may include non-sensitive student personal information such as first name and last initial and student group photos.

Student names and/or photographs may be printed in school yearbooks, school programs or brochures (commencement or graduation programs, school plays and musical productions), on student awards, honour rolls, on class assignment lists and posted throughout the school.

The media, such as newspapers, television and radio may be invited to the school to take photos of students and write articles about newsworthy events or activities including graduations, student achievements / awards, co-curricular activities, sports and current events. Their reports may include group photos of students. Individual students would only be photographed or identified with appropriate consent.

Students participating in extra-curricular activities or school events where the public is invited or that take place in public places such as field trips, malls and fairs, may be photographed by the school community or general public. This may result in photos or recordings being posted on social media sites. The school has no control over how and where these images will be posted; however parents and students are asked to practice good digital citizenship by being respectful when they post photos of others, which includes only posting photos involving other students with permission.

Student information is shared in order to design and deliver programming to meet the needs of all students in our schools. To that end, learning profiles and student achievement levels are shared between staff within a school, in order to best address student needs as they progress through grade levels. As students progress from elementary to secondary school, important information is shared to ease the student's transition to secondary school. Sharing information also improves our ability to program effectively to the benefit of all students. The secondary school will share information about each student's progress throughout secondary school with the student's previous elementary school to support continuous improvement of the elementary school program for all students. Please contact your principal if you would like more information about the transition process.

Secondary schools will send information of potential graduates (contact information, marks and transcripts) to Ontario colleges and universities to support the student's post-secondary applications.

Authorized volunteers or school council members may contact parents on behalf of the school regarding school-related activities which benefit the student and the school community or for the Safe Arrival program.

Student health numbers (OHIP) will not be collected; however, parents/guardians or students may be invited to volunteer such information for students going on field trips.

Student accidents that take place during school or on school sponsored activities will be reported to the board's insurer. Reports include the name of the injured student(s) and details about the incident, as well as the name and contact information of witnesses to the accident. *Personal information* such as child's name, birth date, grade, name of parents/guardians, home address and phone numbers will be shared with the Renfrew County and District Health Unit in accordance with the Immunization of School Pupils Act. Communicable diseases shall be reported in accordance with the Health Promotion and Protection Act and the Education Act.

Ancestry information of First Nation, Métis and Inuit students who chose to voluntarily self-identify will be used to allocate resources, improve student learning and student success and to offer individualized supports and opportunities to students and families. This information will also be reported to the Ministry of Education and the Education Quality Accountability Office (EQAO). Contact your school principal for more information about self-identification.

In keeping with the legislative requirements of the Education Act and Personal Health Information Protection Act*, informed consent will be sought prior to conducting* intelligence or behavioural tests and/or involvement of psychological or speech and language staff. The Renfrew CDSB follows the legislative requirements of the Child and Family Services Act for students accessing social work and/or child and youth work services with regards to informing parent(s)/guardian(s) for students 12 years of age and under prior to accessing services.

Questions

Questions regarding these practices may be addressed to the School Principal or the Superintendent of Educational Services for your Family of Schools at the Board Office (613-735-1031). Please communicate any concerns you have with regards to the sharing of personal information as outlined above by contacting the school principal as soon as possible. The above will apply unless an objection is filed with the principal and an alternative resolution can be found.

[Reprinted from the Simcoe County District School Board, 2015-16 Student Handbook with permission.]

POLICY: Ontarians with Disabilities – Accessibility Commitment

I. Purpose of Policy

The goal of the Accessibility for Ontarians with Disabilities Act (AODA) is to make Ontario accessible to people with disabilities by 1st January 2025 through the identification, elimination and prevention of barriers, to inclusion. AODA has been developed to ensure that all Ontarians with disabilities are treated with respect, dignity and equality.

As an inclusive Catholic educational community, the Renfrew County Catholic District School Board is equally committed to the above goal as part of its mission to nurture the giftedness, self-worth and potential of the whole person.

II. Policy Statement

1. Board Commitment:

The Board is committed to increasing the accessibility for persons with disabilities who study, visit or work in our facilities. We strive to meet the needs of all members of the community in a respectful manner. We will do this by proactively consulting with, and responding to, individuals with disabilities in order to identify and remove recognized and unrecognized barriers

2. Board Actions:

The Board will provide goods, services, resources, facilities, transportation and employment opportunities to persons with disabilities in ways that:

a) recognize and respect their dignity and independence;
b) are integrated as fully as practicable into methods of delivery;
c) ensures reasonable efforts are made to provide an opportunity equal to that given to others who obtain services and who visit and work in our facilities; and
d) allows persons with disabilities to benefit from the same services, in the same place, and in a similar way to other users of our services [the public], applicants and employees.

The Board will continually review internal and external policies, practices and procedures to ensure that we provide accessible services and employment opportunities to all.

III. Definitions

barrier means anything that prevents a person with a disability from fully participating in all aspects of society because of his or her disability, including a physical barrier, an architectural barrier, an information or communications barrier, an attitudinal barrier, a technological barrier, a policy or a practice; ("obstacle")

disability means,

(a) any degree of physical disability, infirmity, malformation or disfigurement that is caused by bodily injury, birth defect or illness and, without limiting the generality of the foregoing, includes diabetes mellitus, epilepsy, a brain injury, any degree of paralysis, amputation, lack of physical co-ordination, blindness or visual impediment, deafness or hearing impediment, muteness or speech impediment, or physical reliance on a guide dog or other animal or on a wheelchair or other remedial appliance or device,
(b) a condition of mental impairment or a developmental disability,

(c) a learning disability, or a dysfunction in one or more of the processes involved in understanding or using symbols or spoken language,
(d) a mental disorder, or
(e) an injury or disability for which benefits were claimed or received under the insurance plan established under the Workplace Safety and Insurance Act, 1997; ("handicap")

IV. Related Information

Related Board Policies

POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Assistive Devices)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Disruption of Service Notice)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Feedback)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Service Animal)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Support Person)

Legislation

Accessibility for Ontarians with Disabilities Act, 2005
Ontario Regulation 429/07 (Accessibility Standards for Customer Service)
Ontario Regulation 191/11 (Integrated Accessibility Standards)

Ministry of Economic Development, Trade and Employment

Making Ontario Accessible

POLICY: Ontarians with Disabilities - Accessibility Standards for Customer Service (Assistive Devices)

Rationale:

In a spirit of freedom, affirmation and celebration, members of the Board Community strive to nurture the giftedness, self-worth and potential of each individual and we reverence the dignity of the whole person, including all persons who interact with our board as customers.

The Board will welcome all members of the school and broader community to our facilities by committing our staff and volunteers to providing services that respect the independence and dignity of people with disabilities. Such services incorporate measures that include but are not limited to the use of assistive devices.

Personnel Affected by Policy:

Trustees, All Board Regular and Occasional Employees and Volunteers

Definitions:

Assistive Device*:* any device used by people with disabilities to help with daily living. Assistive devices include a range of products such as wheelchairs, walkers, white canes, oxygen tanks, electronic communication devices

Customer: any person who uses the services of the Board

Organizational Authority:

The Board

Regulations:

1.0 RESPONSIBILITY

1.1 Supervisory Officers, Principals and Departmental Managers will ensure that staff are trained to support parents and the general public who may use assistive devices while accessing board services.

1.2 Training is focused on how to interact with people using assistive devices rather on the technical use of the assistive devices.

1.3 Students and staff have separate and specific procedures related to their personal use of assistive devices.

2.0 COMMUNICATION RE: USE OF ASSISTIVE DEVICES

Assistive Devices Carried by Persons with Disabilities

2.1 The Board website will indicate that all board facilities provide services that respect the independence and dignity of people with disabilities and offer services that include the use of assistive devices.

2.2 Each Board facility that is open to the public will provide a pamphlet in the front office/reception area that welcomes the use of assistive devices and encourages users to seek support from staff and volunteers as they require it.

Assistive Devices/Services Made available by the Board

2.3 The Board website will indicate the availability of assistive devices provided by the board or school to assist in provision of services to people with disabilities.

2.4 Each Board facility that is open to the public will, as applicable, post information in the front office/reception area in the form of a pamphlet that indicates the availability of assistive devices and encourage potential users to seek support from staff and volunteers as they require it.

2.5 Assistive devices / services made available by the Board could include:

a) assistive devices such as TTY service, telephones with large numbers, amplifiers, lifts;
b) services such as sign language interpretation, oral interpretation, real-time captioning; and
c) alternative service methods such as the assistance of a staff person to complete a transaction, e.g., school registration.

Related Information

Appendix for this Policy

Appendix: Assistive Devices & TTY Information

Related Board Policies

POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Assistive Devices)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Disruption of Service Notice)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Feedback)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Service Animal)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Support Person)

Appendix: Assistive Devices & TTY Information

HELPING SOMEONE WITH AN ASSISTIVE DEVICE

Many users of board services and facilities who have disabilities will have their own personal assistive devices.

Examples of personal assistive devices include:

- wheelchairs,
- scooters
- walker
- amplification devices that boost sound for listeners who are hard-of-hearing without reducing background noise
- hearing aids
- oxygen tanks
- electronic notebooks or laptop computers
- personal data managers
- communication boards used to communicate using symbols, words or pictures
- speech-generating devices that "speak" when a symbol, word or picture is pressed

Key Point To Remember: One should not touch or handle an assistive device without permission.

MOVING PERSONAL ASSISTIVE DEVICES

If you have permission to move a person in a wheelchair remember to:

- wait for and follow the person's instructions;
- confirm that the person is ready to move;
- describe what you are going to do before you do it;
- avoid uneven ground and objects that create bumpy and unsafe ride; and
- practice consideration and safety – do not leave the person in an awkward, dangerous or undignified position such as facing a wall or in the path of opening doors.

Do not move items or equipment, such as canes and walkers, out of the user's reach.

Respect personal space. Do not lean over a person with a disability or lean on their assistive device.

Let the person know about accessible features in the immediate environment (automatic doors, accessible washrooms, etc.).

HOW TO USE TTY AND CANADA RELAY SERVICES

How to make a call with a TTY and the Relay System

1. Push the ON switch
2. Push the DISPLAY switch if you wish to use the screen alone or the PRINT switch if you want what is typed both on screen and in print.
3. Place the telephone receiver on the TTY's rubber receptacles. Make sure that the receiver is firmly in place and that the telephone's receiver cord is on the LEFT side of the TTY.
4. Check the telephone indicator light; if it is lit, you have the line.
5. Dial the number, and watch the telephone light; if it is flashing slowly, this indicates that the device on the other end is ringing.
6. When the person you are calling answers, you will see a phrase appear on the screen such as: "Hello, Richard Smith here, GA." The "GA" stands for "Go Ahead". Don't forget to use it whenever you have finished speaking, so the other person will know it's his or her turn to speak. The person who receives the call is always the one who starts typing first.

POLICY: Ontarians with Disabilities - Accessibility Standards for Customer Service (Disruption of Service Notice)

Rationale:

In a spirit of freedom, affirmation and celebration, members of the Board Community strive to nurture the giftedness, self-worth and potential of each individual and we reverence the dignity of the whole person, including all persons who interact with our board as customers.

When services that are normally provided to a person with a disability are temporarily unavailable such as access to an elevator, a disruption of service notice will be posted at the site and on the Board's website.

Personnel Affected by Policy:

Trustees, All Board Regular and Occasional Employees and Volunteers

Definitions/Explanation of Service Disruption:

As members of the general public, people with disabilities may rely on certain facilities, services or systems in order to access the services of the school or Board offices. Escalators and elevators, for example, are important to people with mobility disabilities because that may be the only way they can access the premises. Other systems and services designed to meet the needs of people with disabilities can include accessible washrooms, amplification systems, and note-taking or TTY services. When those facilities or services are temporarily unavailable or if they are expected to be temporarily unavailable in the near future, a notice of disruption of service is required.

Generally, disruptions to all of the Board's services, such as during a major storm or power outage, do not require this special notice. However, if the disruption has a significant impact on people with disabilities, a notice of the disruption should be provided.

Organizational Authority:

The Board

Regulations:

1. RESPONSIBILITY

Supervisory Officers, Principals, Departmental Managers and designates will ensure that the users of Renfrew County Catholic District School Board and school services are notified when there is a disruption in services that may have an impact on access to services by people with disabilities.

2. HOW MUST THE NOTICE OF DISRUPTION OF SERVICES BE PROVIDED

a) Notice may be given by posting the information at a conspicuous place at or in the school. Other options that may be used include: through direct communication with users of the services in accordance with school practices.

b) Consideration should be given to providing notice in multiple formats.

c) If the disruption is planned, notice should be provided in advance of the disruption. If the notice is unplanned, notice should be provided as soon as possible after the disruption has been identified.

3. WHAT MUST BE INCLUDED IN NOTICE OF DISRUPTION OF SERVICES

The notice of disruption of service must include information about the reason for the disruption, its anticipated duration and a description of alternative facilities or services, if any, that are available.

Related Information

Appendix for this Policy

Appendix: Sample Notices of Disruption of Services

Related Board Policies

POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Assistive Devices)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Disruption of Service Notice)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Feedback)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Service Animal)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Support Person)

-

Appendix: Sample Notices of Disruption of Services

Notice Contents

What Must be Included in Notice of Disruption of Services

The notice of disruption of service must include information about the reason for the disruption, its anticipated duration and a description of alternative facilities or services, if any, that are available.

Sample Notices

Sample 1 – Access to School Building

To: Parents, Guardians and Community Users of our School

Maintenance work will make the main door of the school and the access ramp inaccessible from May 1 to May 8. A temporary ramp has been set up that gives access to the door at the east of the school building. We regret this inconvenience. If you have questions or concerns, please contact _____at [phone number].

Thank you.

Principal

Sample 2 – Accessible Washroom

To: Visitors to the Education Centre

Our accessible washroom is out of service due to a broken pipe. Repairs are underway and the washroom is expected to be usable again by tomorrow. In the interim, we have made arrangements for our visitors to use the accessible washroom at 123 Main Street, which is located next door to our premises. We apologize for this inconvenience.

Thank you.

Superintendent of Facilities

POLICY: Ontarians with Disabilities - Accessibility Standards for Customer Service (Feedback)

Rationale:

In a spirit of freedom, affirmation and celebration, members of the Board Community strive to nurture the giftedness, self-worth and potential of each individual and we reverence the dignity of the whole person, including all persons who interact with our board as customers.

The Board will monitor the effectiveness of implementation of the Accessible Standards for Customer Service through a process for receiving and responding to feedback. Information about the feedback process will be readily available to the public and will allow people with disabilities to provide feedback using a number of methods.

Personnel Affected by Policy:

Trustees, All Board Regular and Occasional Employees and Volunteers

Organizational Authority:

The Board

Regulations:

1. **RESPONSIBILITY**

The Director of Education and/or designate will implement a process for Feedback on Accessible Customer Service that has the following components:

a) Information on the Board and school websites inviting users of Board services to provide feedback on their experience with or concerns about access to services for people with disabilities.

b) A pamphlet available through school offices and public offices of the Board to invite people with disabilities to provide feedback on their experience with or concerns about accessibility of services. Consideration should be given to providing information in alternate formats.

c) Information on how the Board will respond to feedback.

d) The Director of Education and/or designates will create a process for reviewing implementation of the policy on Accessibility Standards for Customer Service.

2. **METHODS FOR FEEDBACK**

a) A range of methods for soliciting feedback will be employed to ensure optimum access to the feedback process by people with disabilities.

b) Methods could include electronic e-mail, verbal or written correspondence.

c) The feedback process should include the title(s) of the person(s) responsible for receiving feedback and indicate how the Board's response to the feedback will be made known.

3. **PROACTIVE MEASURES FOR ACCESSIBLE CUSTOMER SERVICE**

To ensure ongoing efficient and effective adherence to the Board's policy on Accessibility Standards for Customer Service, the Board, its managers and its school-based administrators will take into account the impact on people with disabilities when purchasing new equipment, designing new systems or planning a new initiative.

Related Information

Related Board Policies

POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Assistive Devices)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Disruption of Service Notice)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Feedback)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Service Animal)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Support Person)

POLICY: Ontarians with Disabilities - Accessibility Standards for Customer Service (Service Animals)

Rationale:

In a spirit of freedom, affirmation and celebration, members of the Board Community strive to nurture the giftedness, self-worth and potential of each individual and we reverence the dignity of the whole person, including all persons who interact with our board as customers.

The Board will welcome all members of the school and broader community to our facilities by committing our staff and volunteers to providing services that respect the independence and dignity of people with disabilities, such service to incorporate measures that include but are not limited to the use of service animals.

Personnel Affected by Policy:

Trustees, All Board Regular and Occasional Employees and Volunteers

Definitions:

Service animal: is an animal that is being used because of a person's disability and this is either readily apparent or is supported by a letter from a physician or nurse.

Additional information:

Examples of service animals include dogs used by people who have vision loss, hearing alert animals for people who are deaf, deafened or hard of hearing, and animals trained to alert an individual to an oncoming seizure and lead them to safety. The customer service standard's provisions also apply to animals who provide other services to people with disabilities.

It is "readily apparent" that an animal is a service animal when it is obvious by its appearance or by what it is doing. For example, it may be readily apparent that an animal is a service animal if it is wearing a harness, saddle bags, a sign that identifies it as a service animal or has a certificate or identification card from a service animal training school or an identification card from the Attorney General of Ontario. It may also be readily apparent if a person is using the animal to assist him or her in doing things, such as opening doors or retrieving items.

Organizational Authority:

The Board

Regulations:

1. **RESPONSIBILITY**

   Supervisory Officers, Principals and Departmental Managers will ensure that all staff, volunteers and others dealing with the public are properly trained in how to interact with people with disabilities who are accompanied by a service animal

2. **ACCESS TO BOARD PREMISES**

   a) Any person with a disability who is accompanied by a service animal will be welcomed on Board and/or school premises with his or her service animal and be accompanied by the service animal while on the premises. Access will be in accordance with normal security procedures.

   b) This requirement applies only to those areas of the premises where the public or third parties customarily have access and does not include places or areas of the school or board offices where the public does not have access.

c) Access to classrooms for service animals used by students and staff is covered under separate specific procedures.

3. EXCLUSION OF SERVICE ANIMAL

a) A service animal can only be excluded from access to the premises where this is required by another law. Examples include the *Health Protection and Promotion Act* and the *Food Safety and Quality Act.* This act prohibits service animals in places where food is prepared, processed, or handled (e.g., kitchen of school cafeteria or culinary arts classroom) although service dogs are permitted where food is served and sold (e.g., school cafeteria or lunchroom).

b) Where there is a risk to the health and safety of another person as a result of the presence of a service animal, consideration must be given to options available prior to exclusion of a service animal. An example would be a situation where an individual has a severe allergy to the service animal. It is the Board's expectation that the situation be fully analyzed and all measures to eliminate the risk be considered, e.g. creating distance between the two individuals concerned, making reasonable alterations to schedules, etc.

c) A service animal can be excluded if it is of a breed that is prohibited by law. An example would be the Ontario *Dog Owners' Liability Act* which places restrictions on pit bull terriers.

4. ALTERNATIVE MEASURES IF SERVICE ANIMAL MUST BE EXCLUDED

In the rare instance where a service animal must be excluded, the Board must make every effort to put alternative arrangements in place to provide the services required by the person with a disability. This could involve leaving the animal in a secure area where it is permitted by law and discussing with the person how best to serve them, e.g., a person with a vision disability might need someone (a member of staff or volunteer) to guide them.

5. WHEN IT IS NECESSARY TO CONFIRM AN ANIMAL IS A SERVICE ANIMAL

a) Where an animal is not a trained guide dog and it is not readily apparent that the animal is a service animal, the school or board staff member may ask the person using the service animal for a letter from a physician or nurse confirming that the animal is needed because of a disability. The letter does not need to identify the disability, why the animal is needed or how it is used.

b) Where the person using the service animal regularly attends at the school or Board facility, the principal or departmental manager may request to keep a copy of the letter on file but only as long as required by the circumstances. Alternatively, the person using the service animal may be asked to bring a letter with them on occasions when they visit the premises. The confidentiality of the information in the letter is protected by the *Freedom of Information and Protection of Privacy Act.*

Related Information

Related Board Policies

POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Assistive Devices)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Disruption of Service Notice)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Feedback)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Service Animal)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Support Person)

POLICY: Ontarians with Disabilities - Accessibility Standards for Customer Service (Support Person)

Rationale:

In a spirit of freedom, affirmation and celebration, members of the Board Community strive to nurture the giftedness, self-worth and potential of each individual and we reverence the dignity of the whole person, including all persons who interact with our board as customers.

The Board will welcome all members of the school and broader community to our facilities by committing our staff and volunteers to providing services that respect the independence and dignity of people with disabilities, such service to incorporate measures that include but are not limited to the use of support persons.

Personnel Affected by Policy:

Trustees, All Board Regular and Occasional Employees and Volunteers

Definitions:

Support person: is a person who assists or interprets for a person with a disability who accesses the services of the Board. A support person is distinct from an employee who provides support services to a student or staff person in the system – separate and specific procedures apply.

Additional information:

A support person is an individual chosen by a person with a disability to provide services or assistance with communication, mobility, personal care, medical needs or with access to goods or services. Personal care needs may include, but are not limited to, physically transferring an individual from one location to another or assisting an individual with eating or using the washroom. Medical needs may include, but are not limited to, monitoring an individual's health or providing medical support by being available in the event of a seizure.

The support person could be a paid professional, a volunteer, a friend or a family member. He or she does not necessarily need to have special training or qualifications.

Organizational Authority:

The Board

Regulations:

1. RESPONSIBILITY

Supervisory Officers, Principals and Departmental Managers will ensure that staff receive training in interacting with people with disabilities who are accessing board services accompanied by a support person.

2. ACCESS TO BOARD PREMISES

a) Any person with a disability who is accompanied by a support person will be welcomed on Board and/or school premises with his or her support person. Access will be in accordance with normal security procedures.

b) This requirement applies only to those areas of the premises where the public or third parties customarily have access and does not include places or areas of the school or board offices where the public does not have access.

3. CONFIDENTIALITY

a) Where a support person is accompanying a person with a disability, who is the parent/guardian of a student, for the purpose of assisting in a discussion that may involve confidential information concerning the student, the superintendent, principal or other staff member must first secure the consent of the parent/guardian regarding such disclosure.

b) Consent to the disclosure of confidential information in the presence of the support person must be given in writing by the parent or guardian.

c) The support person must also provide assurance in writing to safeguard the confidentiality of information disclosed in the discussion.

d) A copy of the signed consent document will be retained in the school/board office.

e) If the parent/guardian uses a different support person for subsequent meetings, a new signed consent will be required.

4. SUPPORT PERSONS ACCOMPANYING A PERSON WITH A DISABILITY AT SCHOOL EVENTS FOR WHICH THERE IS AN ADMISSION FEE

Where an individual with a disability who is accompanied by a support person wishes to attend a school, family of schools or board-organized event for which a fee is charged, the notice of the event will include information as to whether support persons will be charged a fee and specify the amount of the fee.

5. WHERE THE BOARD MAY REQUIRE THE PRESENCE OF A SUPPORT PERSON

The Board may require a person with a disability to be accompanied by a support person when on the premises, but only if a support person is necessary to protect the health or safety of the person with a disability or the health or safety of others on the premises.

Related Information

Appendix for this Policy

Appendix: Support Person Involvement Consent Form

Related Board Policies

POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Assistive Devices)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Disruption of Service Notice)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Feedback)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Service Animal)
POLICY: Ontarians with Disabilities – Accessibility Standards for Customer Service (Support Person)

Appendix: Support Person Involvement Consent Form

I, _____ consent to the sharing of confidential information
(name of parent/guardian)
by _____
(name of principal/teacher/other staff member)
related to _____ in the
(name of child/ward)
presence of my support person, _____.
(name of support person)
My support person consents to safeguarding the confidentiality of the information shared.

Affirmation of consent:

Parent/Guardian
Signature _____ Date _____

(Printed Name of Parent/Guardian) _____

I undertake to safeguard the confidentiality of information shared between (school staff) and (parent/guardian) for whom I am a support person.

Support Person
Signature _____ Date _____

(Printed Name of Support Person) _____

Signature of Witness –
Principal/Staff Member _____ Date _____

(Printed Name of Witness) _____

POLICY: Record Retention

I. Purpose of Policy

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) requires school boards to implement reasonable measures to ensure that records are preserved or retained in accordance with record retention schedules. (MFIPPA, s. 4 (1))

II. Policy Statement

1. Commitment

The Renfrew County Catholic District School Board is committed to:

- complying with its statutory and legal responsibilities; and
- following the best practices suggested for public sector organizations which are appropriate.

2. Federal / Provincial Legislation

The Board shall comply with

- federal legislation including the *Income Tax Act*;
- provincial legislation including the *Education Act, Limitations Act, 2002*, *Municipal Freedom of Information and Protection of Privacy Act* and
- other applicable legislation.

3. Legal Duty to Protect Students

Court and tribunal decisions involving child abuse, sexual misconduct and inappropriate behaviour impose obligations on educational organizations to take all reasonable precautions to protect children and youth. Records related to protecting students shall be kept permanently.

4. Best Practices

The Government of Canada, the Government of Ontario and other organizations have published best practices for record retention for school boards to consider.

5. Personal Information

a) Personal information means recorded information about an identifiable individual, including,

i) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

ii) 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,
iii) any identifying number, symbol or other particular assigned to the individual,
iv) the address, telephone number, fingerprints or blood type of the individual,
v) the personal opinions or views of the individual except if they relate to another individual,
vi) 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,
vii) the views or opinions of another individual about the individual, and
viii) 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 (s. 2 (1)).

b) The following Board Policy documents (Schools & Students Policy Category):
- Information (Personal) – Collection, Use & Disclosure Policy,
- Procedure A – Student Information and
- Procedure B – Security Measures

provide guidance to Board employees, trustees, agents, independent contractors and other individuals involved with the Board as to their statutory requirements in the collection, use and disclosure of individuals' personal information including information in pupil records.

c) Records containing or related to personal information are classified as highly confidential and the security measure outlined in Procedure A shall be followed.

6. Annual Review

The Policy documents should be reviewed annually.

III. Related Information

Procedure for this Policy

Procedure A- - Security Measures

Federal Legislation

Income Tax Act

Provincial Legislation

Education Act
Limitations Act, 2002
Municipal Freedom of Information and Protection of Privacy
Personal Health Information Protection Act

Other Information

Archives of Ontario. (23-Jun-08). *Common Records Series for Administrative Functions of the Government of Ontario.*
City of Burlington. (Jan-15). *Records Retention Schedule.*
Personal Information Management (PIM)Task Force. (2008). *PIMtoolkit – Tables of Laws and Citations with Record Retention Requirements for School Boards.*

PROCEDURE A: Security Measures

I. Overview / Procedure Description

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) requires school boards to implement reasonable measures to ensure that records are preserved or retained in accordance with record retention schedules. (MFIPPA, s. 4 (1))

Some records are classified as personal information under the MFIPPA and are highly confidential. This Procedure sets out reasonable security measures and safeguards to protect the above information.

II. Areas of Responsibility

All Board employees, trustees, agents, independent contractors and other individuals involved with the Board must follow these reasonable security measures and safeguards to protect the above information.

III. Procedure Steps / Checklist

1. Workplace Security

a) Paper and electronic files containing personal information shall be kept secure at all times. For example, when transporting records, laptops, CDs, etc. care shall be taken to keep them secure.

b) All documents or files containing personal information shall not be left unattended and left or in open view while in use.

c) The integrity and availability of records shall be preserved by:

i) taking records off-site only when absolutely necessary; whenever practical, the original shall remain on-site and only copies removed. OSRs shall not be removed from the school;

ii) clearly identifying copies of documents containing personal information (for example IPRC packages) and destroying when no longer needed;

iii) using a sign-in/sign-out procedure including a sign out date to monitor removed files;

iv) returning records to a secure environment as quickly as possible, for example, at the end of a meeting or the end of the day.

d) All working copies of paper files containing personal information shall be returned to the office or a secure environment for destruction. Records containing personal or confidential information shall never be discarded in an individual's or a public trash or recycling bin.

e) Visitor access to areas where confidential information is being worked on or is stored shall be controlled. Unknown persons seen in operational areas shall be questioned e.g. Can I help you? Are you looking for someone? etc.

f) Areas of the building where personal information is stored shall be secured after normal business hours.

g) Keys and access to locked file cabinets and locked areas shall be controlled and monitored.

h) When discussing a student, staff shall ensure that the conversations are professional, appropriate and respectful of the audience.

2. Computers and Electronic Information

a) Email messages shall not contain sensitive personal information about an identifiable individual unless absolutely necessary. Where it is necessary to include such information in an email, consider using the individual's initials, symbols or a code rather than a full name to help maintain anonymity of the individual.

b) Computer monitors shall be positioned to minimize unauthorized viewing of the information displayed on the monitors.

c) Monitors displaying personal information shall never be left unattended and password protected screen saver options shall be used during periods of inactivity.

d) Computer hard drives and file storage media should be encrypted and must be secured against improper access by a strong password (alpha, numeric and symbol).

e) Computer hard drives and file storage media must be rendered unusable when disposed of. Contact the Helpdesk for guidance.

3. Mobile Devices

a) Mobile devices include, but are not limited to, board-owned laptops/notebook computers, integrated hand held/Personal Digital Assistants (PDAs), cellular phones removable media (flash drives, memory sticks, removable drives) that are connected to board computing devices and used to store and/or transport information to another device. Do not share or leave file storage media containing personal information unattended. Ensure that it is secured when not in use.

b) All mobile devices must be secured against improper access by a strong password (alpha, numeric and symbol). If the mobile device is used to store personal information, the drive must be encrypted.

c) Laptop hard drives must be encrypted and must be secured against improper access by a strong password (alpha, numeric and symbol). As much as possible personal or sensitive information should not be stored on laptop hard drives. In the event that it is necessary to store data containing personal information on the hard drive of a laptop, password protect the file and try to maintain the anonymity of the individual by initials or codes, etc.

d) Care must be taken when communicating personal information while using a cellular or cordless telephone, as this type of communication can be easily intercepted.

4. Working from Home

Individuals working from home must ensure that they take reasonable steps to protect any personal information they use in their home work location by:

a) designating a secure work area as "office space" which can only be accessed by the individual;
b) storing all work records and sensitive information in the most secure manner possible;
c) using the Board voice messaging system for conducting Board business particularly where personal information is being used;
d) avoiding saving personal work information on home computers;
e) using password protected storage media, or web enabled programs;
f) ensuring that any documents containing personal information that needs to be disposed of is returned to an appropriate work location for shredding and not disposed of in the household garbage.

5. General Privacy Provisions

a) When communicating personal, confidential or sensitive information, consider the physical setting and try to ensure that no one overhears the conversation, i.e. hallways, main office, etc. public telephones, etc.
b) Care must be used when transmitting personal information via a fax machine. If it is necessary to fax highly sensitive personal information, ensure that someone is ready to receive the transmission prior to sending it.
c) When the work environment is not conducive to privacy while collecting or communicating personal information, end and reschedule the conversation or move to a more private environment.

6. Privacy Breaches and Notice

a) A privacy breach occurs when personal information is lost, stolen, or inadvertently disclosed contrary to the *Education Act* or the MFIPPA. This includes the loss of computers, personal devices or media that contain personal information.
b) In accordance with MFIPPA, individuals shall be informed when the security of their personal information is breached.
c) If staff becomes aware of a privacy breach, they must immediately notify their supervisor to ensure that immediate action can be taken to mitigate the impact/results of the breach. For information about responding to a privacy breach, contact your Superintendent.