REPORT TITLE:	**NEW POLICY: PERSONAL INFORMATION MANAGEMENT (PIM)**
REPORT NUMBER:	8. 3) 10-2014
DESTINATION:	Board Meeting #10
DATE:	Wednesday, June 18, 2014
AUTHOR OF REPORT:	Stephen Charbonneau, Superintendent of Education
TYPE OF REPORT:	**ACTION**

Background:

1. The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) requires school boards to have policy in place to address Personal Information Management and Protection of Privacy concerns. At present our board does not have a Personal Information (PIM) Policy.

2. Practices surrounding the creation, use and storage of electronic data, and the designating of a PIM/FOI officer with accountability for all PIM issues, FOI requests, breach reporting, and compliance with standards are two areas of need at present.

3. A PIM Committee was established with representatives from various departments and positions in the board that are involved in the collection, maintenance, storage and disposal of personal information.

4. A number of materials were created by the PIM Taskforce and the following were presented to the Board Policy Review Committee after discussion by the PIM Committee:

    1) Draft policy,
    2) Draft breach protocol,
    3) Model of Records management,
    4) Sample Principal's Handbook.

Comments:

5. The PIM committee received suggestions from the Board Policy Review Committee at the May 14th meeting and provided a final draft at the Board Policy Review meeting on June 11th. The changes made to the newly created Personal Information Management Policy ensure compliance with Ministry requirements.

6. The Board Policy Review Committee recommended that the Board approve of the new policy statement at the June 11th meeting.

7. The new policy statement Professional Standards PS-14 Personal Information Management is provided as **Appendix A.**

8. The breach procedures are enclosed as **Appendix B.**

9. The PIM Committee will continue their work in the development of procedures surrounding the creation, use and storage of electronic data, and the designating of a PIM/FOI officer with accountability for all PIM issues, FOI requests, breach reporting, and compliance with standards.

Recommendation:

10. That the Board approve the new Professional Standards Policy, PS-14 Personal Information Management, as presented.

Simcoe Muskoka Catholic District School Board

Appendix A

PROFESSIONAL STANDARDS

Policy Number PS-14

Personal Information Management

POLICY:

The policy of the Board is to protect the personal information under its control and the individuals' right of privacy regarding personal information that is collected, used, disclosed, and retained in the school system. To this end, this Privacy Policy and its associated procedures are based on globally recognized fair information principles and are grounded in Ontario privacy legislation.

ACCOUNTABILITY AND RESPONSIBILITY:

The Director is accountable for compliance with privacy legislation under the Municipal Freedom of Information and Protection of Privacy Act, and the Personal Health Information Protection Act.

SPECIFIED PURPOSES:

The purposes for which personal information is collected are specified, and individuals are notified of the purposes at or before the time personal information is collected.

CONSENT:

An individual's informed consent is required for the collection, use, and disclosure of personal information, except where otherwise permitted by law.

LIMITING COLLECTION:

The collection of personal information is fair, lawful, and limited to that which is necessary for the specified purposes.

LIMITING USE, RETENTION, AND DISCLOSURE:

The use, retention, and disclosure of personal information are limited to the specified purposes identified to the individual, except where otherwise permitted by law.

ACCURACY:

Ontario school boards/authorities ensure that personal information is accurate, complete, and up-to-date in order to fulfill the specified purposes for its collection, use, disclosure, and retention.

SECURITY SAFEGUARDS:

Personal information is secured and protected from unauthorized access, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.

OPENNESS AND TRANSPARENCY:

Policies and practices relating to the management of personal information are made readily available to the public.

ACCESS AND CORRECTION:

An individual has the right to access his/her personal information and will be given access to that information in accordance with privacy legislation, subject to any restrictions. An individual has the right to challenge the accuracy and completeness of the information and request that it be amended, as appropriate, or to have a letter/statement of disagreement retained on file. Any individual to whom the disclosure has been granted in the year preceding a correction has the right to be notified of the correction/statement. An individual is to be advised of any third party service provider requests for his/her personal information in accordance with privacy legislation.

COMPLIANCE:

An individual may address or challenge compliance with the above principles to the Director (or designated PIM Officer) of the board.

For Approval: Board Meeting #10 (Wednesday, June 18, 2014)

Appendix B

PROCEDURES/GUIDELINES
Supporting
PROFESIONAL STANDARDS

Policy Number PS-14
Personal Information Management

BREACH PROCEDURES

1. RATIONALE:

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) establishes rules for government organizations to follow to ensure the protection of individual privacy. A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with MFIPPA.

2. GENERAL:

2.1 Board staff, upon learning of a breach or suspected breach, shall immediately take the following actions:

2.1.1 contain the breach to stop any more information from being revealed,

2.1.2 assess the extent of the breach,

2.1.3 notify their immediate supervisor and the Freedom of Information, Privacy and Records Information Management Officer, and

2.1.4 complete a Privacy Breach Summary Report.

2.2 Examples of privacy breaches include, but are not limited to: leaving student or staff personal information on a desktop or in a photocopier and a parent or student finds the information; leaving a computer "open" (i.e. logged in or unlocked) and a parent, member of the public or a student is able to view personal information; throwing confidential information in a recycle bin or garbage container; or sending an e-mail to the wrong group of recipients.

3. CONTAINMENT:

3.1 The first step in responding to a privacy breach is to stop the inappropriate flow of data. This may include such actions as taking down a website; retrieving items from garbage bins; "unsending" an e-mail message if possible; calling recipients and asking them to destroy the information; changing a password; looking for a lost computer, memory stick, etc. Record the names and contact information of any persons that received inappropriate information in case there is a need for later follow-up.

4. ASSESSMENT

4.1 Assessing the extent of the breach includes asking questions such as "What data was revealed", "How much data was revealed?", "How sensitive was the data?", "How long has the data been inappropriately available?", "Has the data been reviewed and/or used?", "How did the breach happen?". This information will be of help to the Freedom of Information, Privacy and Records Information Management Officer who must complete a Privacy Breach Summary Report (*cf.* s. 5.3).

5. NOTIFICATION:

5.1 An employee who discovers or suspects a breach must notify his or her immediate supervisor and the Freedom of Information, Privacy and Records Information Management Officer. The Freedom of Information, Privacy and Records Information Management Officer will launch an investigation into the privacy breach and will determine whether notification is required to anyone whose personal information has inadvertently been revealed.

5.2 Depending on the nature and extent of the breach, the Freedom of Information, Privacy and Records Information Management Officer may also notify the Ontario Information and Privacy Commissioner's Office, which may decide to launch its own investigation.

5.3 The Freedom of Information, Privacy and Records Information Management Officer shall submit a Privacy Breach Summary Report to the Director of Education that outlines the causes of the breach, the steps taken to address it, and recommendations for preventing future breaches of a similar nature.

Reviewed:Board Policy Review Committee Meeting #06 (Wednesday, June 11, 2014)

Back to Report