Third-party Privacy Agreements for Outsourced Services

Purpose

The purpose of this guideline is to provide tools that can be used by Ontario school boards and authorities when contracting services that involve the release or use of staff and student personal information to ensure it is protected.

Overview

In accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and the Personal Health Information Protection Act (PHIPPA), Ontario school boards/authorities are required to protect personal information.

Ontario school boards/authorities frequently outsource services by entering into service contracts with other organizations as a means of obtaining value and service for Ontario taxpayers. Such services may include:

- information technology services (e.g., data storage or warehousing, troubleshooting, etc.);
- school bus operators for transportation of students;
- financial services such as payroll;
- records storage and document destruction; and
- conducting research

Under these service agreements, the Ontario school board may transfer custody of student or staff personal information to a third party for the provision of the service. In these cases, while the third party has custody of the information, the board retains control over it and must ensure that the third party meets the board's obligations under the laws of Ontario, including the MFIPPA. This includes ensuring that the information is:

- protected by appropriate safeguards;
- collected, used, disclosed, and disposed of appropriately;
- the school board is notified of potential breaches; and

- the school board is notified of any further transfer of custody of the information to an alternate service provider.

Consideration of the Laws

Education Act

Municipal Freedom of Information and Protection of Privacy Act and Regulations

Personal Health Information Protection Act and Regulations

Definitions

Third Party – any outside individual (e.g., a consultant), business or organization that provides a service to, or acts on behalf of, a school board/authority.

Supporting Standards

Privacy Standard
Privacy Impact Assessment Guidelines

Best Practice Guidelines

To support school boards in outsourcing services, this guideline includes:

1) a risk assessment tool that can be used to assess a third party's privacy and security practices; and
2) model agreements between the service provider and the board.

School boards' Purchasing Services staff, Access and Privacy staff, and the impacted department or school should collaborate to determine the best method for implementing these guidelines for new service agreements.

Additionally, consideration should be given to having existing service providers complete the assessment tool and sign the agreements where an agreement has not previously been completed.

Service Provider Privacy and Security Assessment Tool

This tool is designed to help school boards assess the privacy and security practices of any perspective or current vendor. School boards should incorporate this tool into their tender process where the tender involves personal information. The tool is attached as appendix A.

Privacy Considerations for Confidentiality/Data Sharing Agreements

If the Privacy and Security Assessment is satisfactory and the board is prepared to enter into a contract for service, the board should a) include privacy provisions as part of the service contract or agreement, or b) request that the vendor sign a separate confidentiality or data sharing agreement.

Essentially, the contractual provisions should indicate that any third party to whom personal information is disclosed must maintain safeguards to protect it. Third parties must also protect against unauthorized usage, modification, copying, accessing, or other unauthorized processing of such information. In this regard, the objective is to ensure the security and confidentiality of all records and data, protect against anticipated threats or hazards to the security or integrity of information, and protect against unauthorized access to or use of information.

Where the decision is to include clauses in the service agreement, at a minimum the following clauses should be used:

Collection

Where a third party is collecting personal information on behalf of the school board/authority, it must comply with the provisions regarding the authority to collect, the manner of collection, and notice of collection. See sections 28, 29 (1) and 29 (2) of MFIPPA.

Retention

The third party must adhere to the minimum retention periods for personal information in accordance with S. 5 of MFIPPA Regulation 823 unless the school board specifically provides for a different retention period.

Use and Disclosure

Regardless of how the third party receives the personal information, it must use it in accordance with MFIPPA sections 31 and 32; for example:

- Personal information can only be used or disclosed when the individual to whom the information pertains has identified the information in particular and consented to its use and/or disclosure, or for a purpose for which it was obtained or compiled, or for a consistent purpose.

Disposal

Approved procedures and methods to dispose of personal information in the custody of the third party shall be approved and included in the agreement. Where personal information is in digital format, the agreement should state that the media cannot be re-used unless the information on it can be destroyed in such a way that it cannot be re-created. As a best practice, a school board should have personal information returned to it for disposal via its Records and Information Management program instead of having the third party dispose of it, unless the third party can comply with the requirements of the school board's Records and Information Management program.

Security

Third parties must implement and prove adherence to appropriate precautions to ensure that personal information can be reproduced if the original information is lost or unintentionally destroyed. Once personal information is returned to the school board/authority, the third party must prove that it cannot reproduce that information.

Other Considerations

Accountability

Assign and document accountability within the school board and the third party. Ensure that a reliable plan exists should informational privacy be breached.

Business Continuity

Be prepared should a contractual breach occur, rendering the personal information inaccessible. For example, retain the data in duplicate in a secondary location or in another format.

Training

Ensure that appropriate staff is knowledgeable in the requirements and particulars of third-party privacy agreements.

Ensuring Third-Party Compliance

Include in your agreement that third parties must advise their staff or subcontractors of the privacy provisions both within the legislation and within their contractual obligation. Also require them to sign an undertaking of confidentiality regarding personal information. Boards may also choose to restrict third parties further subcontracting of services without the prior board approval.

Cross-Border Transfer of Personal Information

Many organizations, including school boards, have expressed concerns about having personal information transferred across borders because once the information leaves Canada, only the laws of the receiving country will apply to the information. For example, American companies are subject to U.S. regulation—including the USA Patriot Act, which permits U.S. law enforcement officials, for the purpose of an anti-terrorism investigation, to seek a court order that allows access to the personal records of any person without that person's knowledge, as long as the relevant records are stored in the United States.

There is no law or requirement that prohibits the transfer of personal data across borders; however, investigations by the Ontario Information and Privacy Commissioner (IPC) highlight the IPC's opinion that electronic health records and personal health information should remain in Canada to avoid disclosure of personal information.

Further, with regard to cross-border transfer of OSR information, it is not clear if the OSR "privilege" set out in the Education Act requires school boards to comply with a higher standard to protect the information stored by a third party. Therefore, school boards

should be cautious in their selection of third-party services and providers that will require or permit OSR information or personal health information to cross borders.

When personal information crosses any border, school boards should ensure that all service agreements contain contractual provisions to provide equivalent protection to personal information that is being transferred outside of Canada, including specific controls pertaining to the access to and disclosure of personal information. These service agreements should describe where the personal information will be stored, establish safeguards to ensure information will not be inappropriately access, used, or disclosed, and develop a procedure to respond to a privacy breach.

Model Agreements

Three model agreements are attached as Appendices and can be used where a separate agreement is warranted. The first model agreement can be used to refer to an existing contract or tender, and contains general clauses for protection of information. The second model agreement can be used to define the process and establish specific rules for collection and use of data. The third model agreement can be used where there is a need to evaluate products or services to protect any personal and/or confidential information being exchanged.

Certification of Destruction

To ensure that obsolete data is properly disposed of, schools should consider requesting that the vendor complete and return a certificate of destruction verifying that personal information has been securely disposed of at the end of the lifecycle or returned to the School Board. A model certification of destruction is attached as Appendix __D__.

References

Guidelines for the Protection of Information When Contracting For Services, Office of the Chief Information and Privacy Officer, Ontario Public Service, March 2007.

How to Protect Personal Information in the Custody of a Third Party, Information and Privacy Commission, Ontario, 1998.

http://www.ipc.on.ca/images/Resources/up-num_18.pdf

http://lexpubli.ca/contracts/confidentiality/legal-terms

http://www.edc.ca/english/docs/ca_e.pdf

http://www.canadalegal.com/forms/confidentiality-non-disclosure-agreement.asp

Service Provider Privacy and Security Assessment Tool

This questionnaire shall be completed by all companies/organizations that provide services to the school board, where personal information is involved.

Service Provider (the "Company")	**Service Provided or Role of the Company**

Describe Personal Information ("Data") collected by or disclosed to the Service Provider

ACCOUNTABILITY AND POLICIES

1. Who is responsible for privacy compliance within the organization?

2. Who is responsible for information security within the organization?

3. Please provide a copy of your privacy policy and related procedures or documents providing guidance for staff regarding the appropriate use and safeguarding of personal information.

4. Does every employee commit in writing to follow confidentiality and security standards for handling customer/personal information?

5. Does the organization have a disaster recovery plan? Yes ☐ No ☐

6. Has a privacy assessment, audit and/or security review been performed in the past? By whom? Are these conducted regularly? Please provide available results or information from such assessments, audits or reviews.

7. How frequently does the organization review and update information handling practices and related documentation?

8. Do plans exist to identify security breaches or disclosures of personal information in error?

INFORMATION FLOW

1. Is the information retained in paper format, electronic format or both?

2. Where is the information obtained from the school board stored (in paper and electronic format)?

3. Is the information ever used for purposes unrelated to the services being provided to the school board?

4. Is the information ever merged or matched with other data that has not been provided by the school board? Yes ☐ No ☐

   If so, please explain.

5. Is the information ever provided to a service provider of the organization, a contractor, or any other third party outside of the organization? If so, specify the third parties and the purposes for the sharing of the data with them. What steps have been taken to ensure that the data remains safeguarded?

6. Is the information accessible, processed, or stored outside of Canada?

7. If information is transmitted electronically, is that transmission over secure channels and/or encrypted?

8. How long is the information provided by the school board retained? Specify the retention period for data in both electronic and paper format.

9. If the information is being destroyed or returned to the school board, how is this done (for information in print and electronic form)?

SAFEGUARDS

1. Who within the organization has access to the information? Specify access rights for both paper and electronic information.

2. Does every individual with access require such access in order to service the school board?

3. Can access to and changes to the information be audited by date and user identification?

4. When and how is access to the information revoked?

5. Can the information be accessed remotely by organization staff? What safeguards are in place for remote access?

6. Do you maintain a close inventory of your computers?

7. What technical safeguards are in place to ensure that the school board information in electronic format is protected from loss, theft, unauthorized access, or inadvertent disclosure?

8. What physical safeguards are in place to ensure that hard copies of the information are protected from loss, theft, unauthorized access, or inadvertent disclosure?

9. Does the organization maintain secure backups of the information? How is this done?

10. Is all information erased when disposing of computers, diskettes, tapes, hard drives, or any other electronic media that contains the school board information? How is this done?

11. What methods are used to control and monitor physical access to the organization's premises?

TRAINING AND AWARENESS

1. Do you remind all representatives of the organization with access to school board information of privacy best practices and of the requirement to keep customer information secure and confidential?

2. How is this accomplished?

3. Are employees trained regularly on privacy and security? How often?

Service Provider Privacy and Security Assessment Tool

QUESTIONNAIRE COMPLETED BY:	
Name	Title
Signature	Date
RESPONSES REVIEWED BY:	
Name	Title
Signature	Date

Model Agreement 1

(on board letterhead)

AGREEMENT for the CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

Between

(the Board)

and

[insert name of the Company] (The Company)

WHEREAS the Board wishes the Company to provide, and the Company wishes to provide the services more fully set out in [insert the agreement or P.O. number applicable];

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

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

1. TERM. The term of this agreement shall be the period for which the Company is providing services to the Board that require the Company to have access to and/or

possession of and/or use of personal and/or secret business information under the control of the Board.

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

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

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

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

    b. The Parties agree that at no time will the Company for its own use and/or benefit collect, use and/or disclose personal information about and/or belonging to students of the Board.

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

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

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

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

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

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

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

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

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

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

On Behalf of
[insert name]

date

_____ _____

signature

On Behalf of the Company, [name]

Title [insert]

Individual [insert name]

_____

signature

Model Agreement Two

AGREEMENT FOR DISCLOSURE OF PERSONAL INFORMATION

BETWEEN

hereinafter called the ~~C~~ontractor"

AND

{name of Board}
hereinafter called the ~~B~~oard"

WHEREAS the parties wish to enter into an agreement to share personal information for various purposes;

AND WHEREAS the parties wish to ensure that such data transfers are made in compliance with applicable privacy legislation;

THEREFORE the parties agree as follows:

Definitions

1. The following definitions shall apply to terms found in this agreement:

   i. Personal Data means information about an identifiable individual and includes for the purposes of this agreement **[insert a description of the type of personal data to be shared for the purposes of the agreement]**.

   ii. ~~C~~ollecting Party" shall refer to the party to this agreement responsible for collecting personal data.

iii. "Disclosing Party" shall refer to the party to this agreement responsible for disclosing personal data to the other party.

Purposes of the Data Sharing:

2. Personal data will be transferred from the Board to the Contractor **[optional "or collected by the Contractor on behalf of the Board and transferred to the Board"]** only for the following purposes: **[Insert Purposes below]**

i)
ii)
iii)…

Authority to Share Data:

3. Section(s) **_[Insert applicable sections of Act or Regulation]_____** of **__[Insert Statute or Reg]_____** authorize(s) the Board (or the Contractor on its behalf) to collect personal data for the purposes set out in paragraph 2 .

Use of Personal Data by the Contractor

4. The personal data provided by the Board to the Contractor (or collected on behalf of the Board by the Contractor) shall only be used by the Contractor in compliance with section 31 of the *Municipal Freedom of Information and Protection of Privacy Act (*"MFIPPA") . The Contractor shall not use the personal provided under this agreement for any purpose other than that set out in the Agreement and which is specifically authorized by MFIPPA.

Disclosure of Personal Data by the Contractor

5. The personal data provided by the Board to the Contractor (or collected on behalf of the Board by the Contractor) shall only be disclosed by the Contractor in compliance with s. 32 of MFIPPA. The Contractor shall not disclose the personal data under this agreement for any purpose other than that set out in the Agreement and which is specifically authorized by MFIPPA.

6. More specifically, personal data shall only be disclosed by the Contractor to authorized persons or organizations (hereinafter the "subcontractor") after the Contractor has entered into a contract with the subcontractor to ensure the disclosed personal data is treated in compliance with the provisions of MFIPPA. Specifically, such contract shall contain provisions outlining, the restrictions on use, disclosure, obligations with respect to security and accuracy (including the use of confidentiality acknowledgements by the sub-contractor's employees), retention, access and the return, destruction of data consistent with the terms of this agreement and the law.

Notice Requirement **[Use if contractor will be collecting data on behalf of the Board]**

7. Notice to individuals to whom the personal data relates shall be provided by the Contractor when collecting personal data on behalf of the Board and shall take the following form:

   [Insert appropriate notice language. For example:

   "Personal information collected on this form is collected under s. ____ of the _____Act and shall be used for the following purposes ____[describe purposes]. Questions or comments regarding this collection can be directed to the District School Board Information and Privacy Coordinator at tel. # _____ or in writing to _____[address]____"

   or

   "These premises are under video surveillance for [cite purposes] pursuant to s. ____ of the _____Act and shall be used for the following purposes ____[describe purposes]. Questions or comments regarding this collection can be directed to the District School Board Information and Privacy Coordinator at tel # _____ or in writing to _____[address]____"

Method of Disclosing Data

8. Personal data shall be transferred from the disclosing party to the collecting party in the following manner **[describe the manner, i.e., transfer of photocopies (via secured fax?), shipment of disks, electronic data (use of encryption or other e-security?)]**

Accuracy and Security of Data

9. To ensure compliance with s. 30(2) of MFIPPA the Contractor, when it is the collecting party, shall take all reasonable steps to ensure personal data is kept up to date and communicate any such corrections to the Board where the Board is in possession of incorrect personal data previously provided by the Contractor . Any corrections to personal data forwarded by the Board to the Contractor shall be made immediately by the Contractor.

10. The Contractor shall take all reasonable steps to ensure that personal data provided by the Board shall be securely maintained in order to prevent unauthorized access, loss, theft or disclosure. **[Optional sentence] Without limiting the generality of the forgoing, these measures shall include:_____[describe measures, i.e., locked rooms, locked filing cabinets, confidential fax lines, encryption, firewalls, restricted access protocols, separate physical files, "file sign out" processes, etc.]_____**

11. The Contractor shall ensure that those employees responsible for handling the personal data shall sign an acknowledgment of confidentiality in the form attached as Appendix ~~A~~".

Duration of Data Sharing and Retention of Personal Data

12. This agreement shall commence on _____, and will terminate on _____.

13. To ensure compliance with s.30(1) of the MFIPPA, the personal data collected for the purposes of the Agreement shall be retained for a period of **[Note: this should be used if the Contractor is collecting and/or storing personal data to ensure personal data is kept for the minimum period set out in the regs (i.e., 1 year from use or such shorter time as set out by resolution, unless individual consent has been to destroy it before such time)].**

14. Where the Contractor becomes aware that personal data has become subject to an access request, the Contractor shall take all steps to preserve such personal data until such time as the Board authorizes its return to the Board or its destruction. The Contractor shall immediately forward any request for personal data received to the Board's Information and Privacy Coordinator. Additionally, where required and at the request of the Board, the Service Provider shall assist in locating responsive records within the timelines set out in the legislation.

15. Upon termination of this agreement, the Contractor shall, at the written request of the Board, either return the personal data to the Board or destroy the data in compliance with the terms of MFIPPA upon Board authorization. If authorized to destroy the data, such destruction shall comply with the terms of MFIPPA. **[Optional sentence] Specifically, the Contractor shall _____[cite specific measures, i.e., shredding hardcopies, erasing disks/hard drives, etc.]___**

16. If the personal data is to be disposed of, the Contractor shall provide written confirmation of disposal once completed.

Indemnification

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

Amendments

18. The parties may mutually agree to amend this agreement from time to time. Any such amendments shall comply with the terms of MFIPPA.

Survival

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

Signed on behalf of each party by their duly authorized officers this _____ day of _____ , 201__

On behalf of [Name]

[Name of Signator]
[Title]

_____
signature

On behalf of the Contractor, [Name of Contractor]
[Name of Signator]
[Title]

_____

~~-~~Agreement Two – Schedule A"

Acknowledgement of Confidentiality

I, _____ understand that as part of my position, I may be required to handle personal information provided to my employer by the District School Board (the ~~-~~Board") or collected by my Employer on behalf of the Board. I understand that this information is subject to regulation under the *Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA").* I understand and agree that I will limit my use and/or disclosure of such information to those purposes expressly authorized by the Board. Further, I understand and acknowledge the obligations upon my employer under its agreement with the Board and pursuant to the provisions of MFIPPA with respect to access, security, confidentiality, retention, and disposal of personal information and shall comply with such obligations.

Confidentiality and Non-Disclosure Agreement
For Business/Service Evaluation Purposes

Date:

Disclosing Party: Receiving Party:

Subject Matter:

Purpose of Disclosure:

The Disclosing Party is willing to provide access to the Receiving Party of confidential information of the Disclosing Party for the purpose outlined above. In consideration thereof, the parties agree as follows:

A. During the discussion of a possible business or contractual relationship between the parties or in the performance of contractual obligations, the parties may disclose information orally, in writing or by other means and media, to each other about their respective operations and business, including without limitation, computer programs, know-how, processes, ideas, inventions and business, financial and product development plans and strategies as well as any other information clearly communicated to the receiving party as confidential and/or proprietary and all of the aforedescribed information is essential to the disclosing party's conduct and operation of its business and which information is confidential and proprietary information to the disclosing party (~~"C~~onfidential Information").

B. Each party is willing to provide the Confidential Information to the other on the condition that the receiving party holds the Confidential Information in confidence on the terms and conditions hereinafter set forth.

NOW THEREFORE, in order to induce the other party to provide it with the Confidential Information and for other good and valuable consideration, each party hereby warrants, represents and agrees as follows:

1. Confidentiality. The party receiving the Confidential Information (~~"R~~eceiving Party") hereby agrees to hold in the strictest confidence any and all Confidential Information provided by the other party (~~"D~~isclosing Party").

2. Non-Disclosure. The Receiving Party hereby agrees that neither it nor its employees or agents will reveal, duplicate, or otherwise make available the Confidential Information other than to its own employees or agents' employees who have a business need to know and other than is reasonably necessary for the purposes of this Agreement and the performance of contractual obligations under separate agreements.

3. No License. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in any Confidential Information disclosed to the Receiving Party.

4. No Obligation. The furnishing of Confidential Information under this Agreement does not obligate either party to enter into any further agreement or negotiation with the other or to refrain from entering into an agreement or negotiations with any other party.

5. Termination. This Agreement shall continue in effect until terminated by either party in writing. However, the obligations hereunder with respect to any disclosures made while this Agreement is in effect will continue indefinitely thereafter. Each party shall, upon request of the other, return or destroy any and all of the Disclosing Party's Confidential Information that is or has been in its possession and shall retain no copies of the Disclosing Party's Confidential Information.

6. Provisions Inapplicable. Confidential Information does not include information:

(a) that is now, or in the future becomes, freely available to the public through no fault of or action by either Receiving Party;

(b) that was in possession of Receiving Party prior to the time of disclosure by the Disclosing Party or that is independently acquired or developed by the Receiving Party without the aid, application or use of the Confidential Information;

(c) that is obtained by Receiving Party in good faith without knowledge of any breach of a secrecy arrangement from a third party;

(d) that is disclosed with the written approval of the Disclosing Party; or

(e) that is required to be disclosed by law or court order; provided that the Disclosing Party is notified thereof promptly in writing in order to allow the Disclosing Party an opportunity to take reasonable steps in response thereto.

7. Miscellaneous

(a) The Confidential Information is provided on an ~~A~~AS IS" basis. The Disclosing Party makes no warranties, express or implied, with respect to the Confidential Information. The Disclosing Party shall not be liable for any damages incurred by the Receiving Party arising out of use of Confidential Information. Neither party shall be liable to the other party for any special, indirect or consequential damages, including but not limited to, lost savings and lost profits, even if the parties have knowledge of the possibility of such damages.

(b) Failure of either party hereto to enforce at any time any provision of this Agreement or to exercise any right provided herein shall not in any way be construed to be a waiver of such provision or right nor in any way affect the validity of this Agreement or limit, prevent or impair the right of either party subsequently to enforce such provision or exercise such right.

(c) Each party agrees further that it will not (without the prior written consent of the Discloser) for a period of 12 months from the date of this agreement, directly or indirectly, in any manner whatsoever, including, without limitation, either individually or in conjunction with any other Person, as principal agent, shareholder, or in any manner whatsoever use the Confidential Information to carry on or be engaged in or be concerned with or interested in a business which is reasonably similar to the current or planned Business of the Recipient. (a –Competitive Business").

(d) This Agreement shall not be assigned by either party without the prior written consent of the other party.

(e) Each party agrees that improper disclosure by it of the Confidential Information relating to the other party shall result in irreparable damages to the Disclosing Party, and that, in the event that either party is required to bring an action to enforce the provisions of this Agreement, such party shall be entitled to equitable relief, including a preliminary injunction, in addition to all other relief.

(f) In the event that either party hereto deems it necessary to pursue any proceedings to enforce the provision of this

Agreement, the party prevailing in such proceedings shall be entitled to recover from the other party reasonable attorneys' fees, court costs and other expenses incurred therein.

(g) This Agreement shall be construed and enforced in accordance with the internal, substantive laws of the Province of Ontario, but without regard to conflicts of law principles thereof.

Disclosing Party	Receiving Party
By:	By:
Name: Title:	Name: Title:
Date:	Date:

Board logo

CERTIFICATE OF DESTRUCTION OR RETURN

OF {SCHOOL BOARD DATA}

The undersigned,_____(~~-~~SUPPLIER"), certifies that all **(" Board")** data provided to SUPPLIER together with any materials in any form that incorporate, reference, or contain any **Board** data, have been destroyed or returned to the board. The SUPPLIER certifies that this represents all of the **Board's** data in the SUPPLIER'S possession or under its control, including subsequent copies made thereof, copies electronically stored or maintained. No copies will be retained, and any source data media will be immediately returned to the **Board**.

Authorized Signature:_____

Print or Type Name:_____ Title:_____

Date:_____

Specify Return or Method of Destruction:

Recipient of Returned Data (Name and Address):_____

Date of return/destruction:_____ Method of delivery/destruction:_____