OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

PROCEDURE PR.669.GOV

TITLE: PRIVACY BREACH

Date Issued: 29 June 2010
Date Revised:
Authorization: Senior Staff: 29 June 2010

1.0 OBJECTIVE

Every person acting on behalf of the Ottawa-Carleton District School Board (the "District") shall make a reasonable effort to protect personal information in his/her custody or under his/her control, and to immediately notify and contain a privacy breach through a prompt, reasonable and coordinated effort as outlined in this procedure.

2.0 DEFINITIONS

In this procedure,

2.1 **Privacy breach** means an infraction or violation with respect to the collection, use, disclosure, retention, destruction or security of personal information that is inconsistent with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), *Personal Health Information Protection Act* (PHIPA), and the Board's privacy policy and procedures.

2.2 **Person** means an employee, a volunteer, or a trustee of the Ottawa-Carleton District School Board, or a third-party service provider who is in possession of personal information collected or held by or on behalf of the District.

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

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

b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

c) any identifying number, symbol or other particular assigned to the individual,

d) the address, telephone number, fingerprints or blood type of the individual,

e) the personal opinions or views of the individual except if they relate to another individual,

f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

g) the views or opinions of another individual about the individual,

h) 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.

Personal information does not include information about an individual who has been dead for more than thirty years.

2.4 **Personal health information** means identifying information about an individual in oral or recorded form, if the information,

a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,

b) 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,

c) is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual,

d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,

e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,

f) is the individual's health number, or

g) identifies an individual's substitute decision-maker.

Personal health information does not include information about an individual who has been dead for more than fifty years.

2.5 **Third party service providers** means any outside individual (such as a consultant), a business or an organization that provides a service to, or acts on behalf of, the District. For the purposes of privacy breach reporting, it includes all contractors that receive personal information for the district or collect personal information on behalf of the District, such as school photographers, bus operators, administrators or professional service providers.

3.0 RESPONSIBILITY

Director's Executive Council; Freedom of Information Coordinator (FOI Coordinator); principals; managers; supervisors; and District's Legal Advisor. Specific responsibilities are outlined below and referenced in Appendix B through a summary of roles and responsibilities in responding to a privacy breach.

4.0 PROCEDURE

Every person shall protect personal information in his/her custody or under his/her control, and shall immediately notify and make every effort to contain a privacy breach, in accordance with the provisions of this procedure. A privacy breach has occurred when there is an inappropriate collection, disclosure, use, retention, disposal or security of personal information.

In the event of a privacy breach, the following actions must be undertaken by the identified individuals.

5.1 Every person will be responsible for:

a) Reviewing the five step response protocol outlined in this procedure;

b) As soon as a privacy breach or suspected privacy breach is discovered, notifying his or her supervisor immediately, or in his/her absence, the Freedom of Information (FOI) Coordinator;

c) Containing, if possible, the suspected privacy breach by suspending the process or activity that caused the privacy breach; and

d) Working with their supervisor and/or the FOI Coordinator, to ensure details of the privacy breach and corrective actions are documented, using OCDSB 669-Privacy Breach Report (refer to Appendix C).

5.2 All supervisory officers, managers and principals will be responsible for:

a) Reviewing the five step response protocol outlined in this procedure;

b) Obtaining all available information about the nature of the privacy breach or suspected privacy breach, to determine what happened;

c) Alerting the FOI Coordinator and providing as much information about the privacy breach as is currently available;

d) Working with the FOI Coordinator to undertake all appropriate actions to contain the privacy breach;

e) Working with the FOI Coordinator to ensure details of the privacy breach and corrective actions are documented, using OCDSB 669 - Privacy Breach Report (refer to Appendix C);

f) Notifying, as required, individual(s) whose personal information was breached, following confirmation from the FOI Coordinator;

g) Leading the internal investigation reports and recommending required remedial and corrective actions; and

h) Working with the FOI Coordinator to implement the activities associated with corrective actions as approved and/or directed by the Information and Privacy Commissioner.

5.3 The Freedom of Information (FOI) Coordinator will be responsible for:

a) Reviewing the five step response protocol outlined in this procedure with the superintendent, supervisor, manager or principal to confirm who will be responsible for next steps and timelines;

b) Supporting the superintendent, supervisor, manager or principal in responding to the privacy breach;

c) Notifying the Information and Privacy Commissioner of Ontario where appropriate;

d) Ensuring that those whose personal information has been compromised are informed as required;

e) Briefing senior management, the Director of Education and the Board of Trustees as necessary and appropriate;

f) Reviewing internal investigation reports and identifying required remedial action;

g) Responding to questions from the public regarding the privacy breach; and

h) Monitoring implementation of any required remedial action.

5.4 The third party service providers will be responsible for:

a) Informing the District contact as soon as a privacy breach or suspected privacy breach is discovered;

b) Reviewing the five step response protocol outlined in this procedure;

c) Taking all necessary actions to contain the privacy breach as directed by the District contact and/or FOI Coordinator;

d) Working with the FOI Coordinator and/or District contact, to document how the privacy breach was discovered, what corrective actions were taken and report back, using OCDSB 669 - Privacy Breach Report (refer to Appendix C);

e) Undertaking a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;

f) Taking all necessary remedial action to decrease the risk of future privacy breaches; and

g) Fulfilling contractual obligations to comply with privacy legislation.

5.0 PRIVACY BREACH RESPONSE PROTOCOL

The following protocols shall be initiated as soon as a privacy breach or suspected privacy breach has been reported. The Privacy Breach Report - OCDSB 669 – shall be used to document the privacy breach and provide a guide for the privacy breach management process. Depending on the severity of the privacy breach, some activities may be carried out simultaneously, in quick succession and / or by various individuals as noted in this procedure.

5.1 STEP 1 – RESPOND, REPORT AND ASSESS

In the event of a potential breach of personal information, or when a privacy breach is identified by an internal or external source, every person shall:

a) Assess the situation to determine if a privacy breach has indeed occurred and what needs to be done. If the situation involves personal information and unauthorized collection, use, disclosure, retention or security of personal information, it can be assumed that a privacy breach has occurred and shall be reported.

b) Report the privacy breach to key persons within the District (i.e. your immediate supervisor, the Director of Education, the FOI Coordinator, the Legal Advisor, and the Manager of Business and Learning Technologies) and, if necessary, to law enforcement.

c) Receive advice from your supervisor and the FOI Coordinator on appropriate steps to take to respond to the privacy breach.

d) Document the privacy breach and response activities. Once the breach has been resolved, evaluate the effectiveness of the response to the privacy breach and implement improvements as necessary.

5.2 STEP 2 – CONTAIN

Immediately upon the discovery or external reporting of a privacy breach, or following discussion with the FOI Coordinator and confirmation that a privacy breach has occurred, every person shall:

a) Identify the scope of the privacy breach and contain it (e.g. retrieve the hard copies of any personal information that has been disclosed, determine if the breach would allow unauthorized access to any other personal information (e.g. electronic information system), change passwords and identification numbers and/or temporarily shut down the system if necessary to contain the privacy breach).

b) If the privacy breach involved the provision of personal information to an individual other than who the information belongs to, and without the required consent for the provision of this information, every attempt should be made to receive a signed “Privacy Breach Acknowledgement” – OCDSB 670 - from the individual who incorrectly received the personal information. (Refer to Appendix D). The individual is not obligated to sign the acknowledgement, however, as part of the containment stage, may cooperatively agree to provide the signed

form. If it is determined necessary to inform the individual whose privacy was compromised, he/she should be informed if the Acknowledgement form was secured by the District.

c) Document the privacy breach and containment activities.

d) Develop briefing materials if requested in addition to the Privacy Breach Report – OCDSB 669.

e) Brief the FOI Coordinator, the applicable supervisory officer and key persons about the privacy breach and how it is being managed.

5.3 STEP 3 – INVESTIGATE

a) Once the privacy breach is confirmed and contained, and in cooperation and collaboration with the employee's supervisor, manager or principal, and under the direction of the FOI Coordinator, every person shall:
   (i) Identify and analyze the events that led to the privacy breach;
   (ii) Evaluate what was done to contain it;
   (iii) Recommend remedial action so future privacy breaches do not occur; and
   (iv) Document the results of internal investigation and use the privacy breach report form for record keeping, including:
      (A) Background and scope of the investigation;
      (B) Legislative implications;
      (C) How the assessment was conducted;
      (D) Source and cause of the privacy breach;
      (E) Inventory of the systems and programs affected by the privacy breach;
      (F) Determination of the effectiveness of existing security and privacy policies, procedures and practices;
      (G) Evaluation of the effectiveness of the District's response to the privacy breach;
      (H) Findings including a chronology of events and recommendations of remedial actions; and
      (I) The reported impact of the privacy breach on those individuals whose privacy was compromised.

5.4 STEP 4 – NOTIFY

Considerations for Determining if Notification is Required:

a) Upon being made aware of a privacy breach, the FOI Coordinator shall determine whether notice is required, to whom, when and how.

b) The FOI Coordinator, in conjunction with the supervisor, shall determine who will notify the individual(s) whose personal information was disclosed.

c) In determining whether notice is required, the FOI Coordinator shall consider the following factors:

(i) Risk of Physical Harm – Consideration shall be given to the loss or theft of information place any individual at risk of physical harm, stalking, or harassment.

(ii) Risk of Hurt, Humiliation, or Damage to Reputation – Consideration shall be given to the loss or theft of information lead to hurt, humiliation, or damage to an individual's reputation. This type of harm can occur with the loss or theft of information such as mental health records, medical records, or disciplinary records.

(iii) Risk of Identify Theft – Consideration shall be given to the level of risk of identity theft or other fraud. Identity theft is a concern if the privacy breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).

(iv) Risk of Loss of Business or Employment Opportunities – Consideration shall be given to whether the loss or theft of information could result in damage to an individual's reputation, affecting his/her business or employment opportunities.

(v) Who Had Access to the Breached Personal Information – Consideration shall be given to the recipient of the personal information for example individuals that are bound by professional duties of confidentiality or members of colleges that may be sanctioned if confidentiality is breached.

(vi) Reasonable Expectations – The affected individual's reasonable expectation of notification shall be considered.

<u>Notification Shall Include:</u>

a) The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:

(i) What happened (description of the incident, timing and information involved);

(ii) The nature of potential or actual risks or harm;

(iii) What mitigating actions the District is taking;

(iv) Appropriate action for individuals to take to protect themselves against harm;

(v) A contact person, such as the FOI Coordinator, for questions or to provide further information.

b) If personal information that could lead to identify theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's right to complain to the IPC about the District's handling of their personal information, along with contact information for the IPC.

<u>Notification Timeline:</u>

Affected individuals shall be promptly notified. Depending on the nature and scope of the privacy breach and status of the investigation, notification may occur in stages.

Method of Notification:
The method of notification shall be guided by the nature and scope of the privacy breach and in a manner that reasonably ensures that the affected individual will receive it. Direct notification (phone, letter, e-mail or in person) is preferable and shall be used where the individuals are identified. Where it is not possible to determine the affected individuals, for example when a student information system has been breached, posted notices, media releases, website notices or letters to students or staff shall be considered.

Notification Responsibility:
Notice should not be made prior to confirmation from the FOI Coordinator that notice is required, to whom, when and how. Ideally the individual(s) shall be notified by the supervisor of the employee / department associated with the privacy breach. For example, where the breach is for student information, the principal of the school shall be responsible for providing notification; or where the breach is for staff information, Human Resources shall be responsible. The FOI Coordinator may be referred to as a contact for questions.

Notification to Authorities or Organizations:
Depending on the breach, examples of organizations that may need to be notified include: police if theft or other crime is suspected; insurers; Information and Privacy Commissioner, as appropriate; credit card companies and financial institutions, third party contractors or other parties that may be affected; other departments or staff; or, union or other employee groups.

5.5 STEP 5 – IMPLEMENT CHANGE

The extent of the implemented change and corrective actions required shall be determined by the significance of the privacy breach and whether it was systemic or isolated. Corrective action undertaken by the employee, the supervisor, manager or principal, in conjunction with the FOI Coordinator, might include the following activities:

a) Review the relevant information management systems to enhance compliance with privacy legislation.

b) Amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information.

c) Develop and implement new security or privacy measures, if required.

d) Review employee training on legislative requirements, security and privacy policies, procedures, and practices to reduce potential or future privacy breaches, and strengthen as required.

e) Test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified.

f) Recommend further remedial action to the FOI Coordinator.

6.0 APPENDICES

Appendix A – Examples of privacy breaches
Appendix B – Roles and Responsibilities in Responding to Privacy Breaches - Summary
Appendix C – OCDSB 669 - Privacy Breach Report Form
Appendix D – OCDSB 670 – Privacy Breach Acknowledgement
(Sample forms only – Refer to the OCDSB Forms Conference on BEAM for the most current version of the forms)

7.0 REFERENCE DOCUMENTS

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56
Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Regulation 823
Personal Health Information Protection Act, 2004, SO, c. 3
The Education Act, R.S.O. 1990, Chapter E.2
Privacy and Information Management PIM Taskforce and Toolkit September 2008
Board Policy P.128.GOV: Privacy Policy

OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Appendix A
PR.669.GOV

Personal information can be compromised in many ways. Some privacy breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error, such as an individual's personal information being sent by mistake to another individual (e.g., fax number, e-mail address, etc.). In today's environment in which technology increasingly facilitates information exchange, sometimes a privacy breach can be more wide-scale, such as when an inappropriately executed computer programming change causes the personal information of many individuals to be compromised.

Privacy beaches may be relatively obvious while others may not be as apparent. A privacy breach has occurred when there is an inappropriate collection, disclosure, use, retention, disposal or security of personal information. General examples include:

- Lost or misplaced personal information;
- Stolen technologies or equipment that may contain personal information;
- Disclosure of personal information to an unauthorized person or group;
- Deliberate disclosure of personal information to an unauthorized person or group for fraudulent or other purposes;
- Information used for a purpose not consistent with the reason the information was collected; or
- Information collected in error.

THE FOLLOWING ARE SOME SPECIFIC EXAMPLES OF PRIVACY BREACHES:

	Student Records	**Employee Records**	**Business Records**
Inappropriate collection / disclosure or use of personal information	Two teachers discussing (and identifying) a student in the local grocery store. Student's report card mailed to the wrong home address. Digital images of individuals taken and displayed without consent. Hard-copy psychological assessments kept in openly accessible file cabinets that are not secured or controlled. Ontario Student Records lost	Budget reports (containing employee numbers and names) found in their entirety in recycle bins and garbage bins. Theft from car of a briefcase containing a list of home addresses of teaching staff.	A list of names, including credit card numbers, left on the photocopier. Personal information disclosed to trustees who did not need it to effectively decide on a matter.

	during a transfer from one school to another. Confidential student health records inadvertently blown out of a car trunk and scattered over a busy street.		
	Student Records	**Employee Records**	**Business Records**
Technology/ computer error	Lost memory key or USB stick containing student data. Theft from teacher's car of a laptop containing Special Education student records on the hard drive.	Sending very sensitive personal information to an unattended, open-area printer. Password written on a sticky note stuck to a monitor, which results in the access and disclosure of personal information through malicious actions of another individual accessing the computer. Resumes faxed or e-mailed to a wrong destination or person.	Stolen laptop containing names and addresses of permit holders. Tender information scanned and not cleared from multifunctional office machine. Disposal of equipment with memory capabilities (e.g., memory keys, disks, laptops, photocopiers, fax machines, or cell phones) without secure destruction of the personal information it contains.

OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

ROLES AND RESPONSIBILITIES IN RESPONDING TO PRIVACY BREACHES

REFER TO *PR.669.GOV – PRIVACY BREACH* PROCEDURE FOR INFORMATION ON THE FIVE STEP RESPONSE PROTOCOL.

The following individuals shall be involved when the District responds to a privacy breach. Some of the following roles and responsibilities may be undertaken concurrently.

Individuals	Roles	Responsibilities
Employees, Trustees, Volunteers	All Ontario school board employees need to be alert to the potential for personal information to be compromised, and therefore potentially play a role in identifying, notifying, and containing a breach. Employees dealing with student, employee and/or business records need to be particularly aware of how to identify and address a privacy breach.	Every person will be responsible for: • Reviewing the five step response protocol outlined in PR.669.GOV; • As soon as a privacy breach or suspected privacy breach is discovered, notifying his or her supervisor immediately, or in his/her absence, the Freedom of Information (FOI) Coordinator; • Containing, if possible, the suspected privacy breach by suspending the process or activity that caused the privacy breach; and • Working with their supervisor and/or the FOI Coordinator, to ensure details of the privacy breach and corrective actions are documented, using OCDSB 669- Privacy Breach Report.
Supervisory Officers, Managers, and Principals	Supervisory officers, managers, and principals are responsible for alerting the FOI Coordinator of a breach or suspected breach and will work with the coordinator to implement the five	All supervisory officers, managers and principals will be responsible for: • Reviewing the five step response protocol outlined in

Individuals	Roles	Responsibilities
	steps of the response protocol.	PR.669.GOV; • Obtaining all available information about the nature of the privacy breach or suspected privacy breach, and determine what happened; • Alerting the FOI Coordinator and providing as much information about the privacy breach as is currently available; • Working with the FOI Coordinator to undertake all appropriate actions to contain the privacy breach; • Working with the FOI Coordinator to ensure details of the privacy breach and corrective actions are documented, using OCDSB 669 - Privacy Breach Report; • Notifying, as required, individual(s) whose personal information was breached, following confirmation of notification from the FOI Coordinator; • Leading the internal investigation reports and recommend required remedial and corrective actions; and • Working with the FOI Coordinator to implement the activities associated with corrective actions as approved and/or directed by the Information and Privacy Commissioner.
Freedom of Information Coordinator (FOI Coordinator)	The FOI Coordinator plays a central role in the response to a breach by ensuring that all five steps of the response protocol are implemented.	The Freedom of Information (FOI) Coordinator will be responsible for: • Reviewing the five step response protocol outlined in

Individuals	Roles	Responsibilities
	The responsibility for protecting personal information affected by a privacy breach is assigned to an identified position who is the accountable decision maker. This individual is the key decision maker in responding to privacy breaches and therefore needs to be familiar with the Ontario school boards/ authorities' roles, responsibilities and the response plan.	PR.669.GOV with the superintendent, supervisor, manager or principal and confirm who will be responsible for next steps and timelines; • Supporting the superintendent, supervisor, manager or principal in responding to the privacy breach; • Notifying the Information and Privacy Commissioner where appropriate; • Ensuring that those whose personal information has been compromised are informed as required; • Briefing senior management, the Director of Education and the Board as necessary and appropriate; • Reviewing internal investigation reports and approve required remedial action; • Responding to questions from the public regarding the privacy breach; and • Monitoring implementation of any required remedial action.
Third Party Service Providers	Increasingly, Ontario school boards/ authorities use contracted third party service providers to carry out or manage programs or services on their behalf. Typical third party service providers are commercial school photographers, bus companies, external data warehouse services, outsourced administrative services (such as cheque production, records storage and shredding),	The third party service providers will be responsible for: • Informing the District contact as soon as a privacy breach or suspected privacy breach is discovered; • Reviewing the five step response protocol outlined in PR.669.GOV; • Taking all necessary actions to contain the privacy breach as directed by the District contact and/or FOI Coordinator;

Individuals	Roles	Responsibilities
	Children's Aid Societies (CAS), Public Health Units (PHU), external researchers, and external consultants. In such circumstances, Ontario school boards/authorities retain responsibility for protecting personal information in accordance with privacy legislation. Therefore, third party service providers need to know their roles and responsibilities if a privacy breach occurs when they have custody of personal information. All third party service providers must take reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements, and are required to inform their respective Ontario school boards/authorities of all actual and suspected privacy breaches.	• Working with the FOI Coordinator and/or District contact, to document how the privacy breach was discovered, what corrective actions were taken and report back, using OCDSB 669 - Privacy Breach Report; • Undertaking a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations; • Taking all necessary remedial action to decrease the risk of future privacy breaches; and • Fulfilling contractual obligations to comply with privacy legislation.

OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Privacy Breach Report
Municipal Freedom of Information and Protection of Privacy Act

(References: P.128.GOV and PR.669.GOV)

BREACH REPORT # _____

Take immediate action when you become aware of or have been advised of a suspected privacy breach.

Review the Privacy Breach Procedure PR.669.GOV for specific information on what defines a privacy breach, roles and responsibilities and the five step response protocol.

Responsibility to initiate this report is held with the person and his/her supervisor where the privacy breach has occurred. Completion of the report can be done in consultation with and under the direction of the Freedom of Information (FOI) Coordinator. Once finalized, the report should be submitted in a timely fashion, in hard copy and electronic form, to the FOI Coordinator who will require the information for reporting the privacy breach to the Information and Privacy Commissioner of Ontario.

STEP 1 – RESPOND, REPORT AND ASSESS

Name of person reporting suspected privacy breach (please print) Date

Job title and work location | Telephone and E-mail

Supervisor | Person incident reported to

Date and time incident discovered

There was a privacy breach due to the inappropriate:

- ❒ Collection of personal information
- ❒ Disclosure of personal information
- ❒ Use of personal information
- ❒ Retention of personal information
- ❒ Disposal of personal information
- ❒ Security of personal information
- ❒ Other

_____

_____

_____

What happened, providing a detailed description of the event?

Where? When?

How was it discovered? Action taken, if any

Was personal information involved? Has an unauthorized breach occurred?

If you answer yes to both questions, follow the privacy breach procedure and complete this form.
If not, no further action is required.

STEP 2 – CONTAIN

Describe any actions taken to limit or contain the breach, for example “shut down the system”, “retrieve copies of records”, “Privacy Breach Acknowledgement form signed and returned” etc.

By whom? Date and Time:

STEP 3 – INVESTIGATE

Who was affected, staff, students, contractors? Approximately how many individuals?

Describe the events that lead to the privacy breach and what form the breach took.

How was the information breached?

STEP 4 – NOTIFICATIONS

No notice should be made until consultation with and directed by the Freedom of Information Coordinator who will confirm who should be notified, when and how.

Who should be notified (determined by the breach)?		*Notification to affected individuals shall include:*	
	Affected individuals		Description of the incident and timing
	Police if theft or other crime is suspected		Description of the information involved
	Insurers or others		Nature of potential or actual risks or harm
	Information and Privacy Commissioner (IPC)		Description of mitigating actions taken
	Credit card companies, financial institutions		Appropriate action for individuals to take to protect themselves against harm
	Third-party contractors or other parties that may be affected		A contact person for questions or to provide further information
	Other departments or staff		Contact information for the IPC, if required
	Union or employee bargaining groups		

Notification was provided by:_____

Date: _____
How:_____

STEP 5 – IMPLEMENT CHANGE

Taking into consideration the steps and activities outlined in the Privacy Breach procedure, describe the steps taken to prevent further problems or privacy breaches:

_____

_____

_____

_____

_____

ACKNOWLEDGEMENT

Report completed by:

_____

Print Name Title Signature

The Director of Education or designate (e.g., Freedom of Information Coordinator) is required to sign below to formally acknowledge that the privacy breach was handled in accordance with privacy legislation and with the Ottawa-Carleton District School Board's privacy policies and procedures:

Print Name	Title	Signature

Date

OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Privacy Breach Acknowledgement
Municipal Freedom of Information and Protection of Privacy Act
(References: P.128.GOV and PR.669.GOV)

BREACH REPORT # _____
(To be completed by the FOI Coordinator)

I, _____, hereby acknowledge that I did receive personal information pertaining to a third party. I understand that this information was provided to me in error and was not intended for my use. I am not responsible for the error in releasing this information, however, I understand that this information is confidential and any distribution, use or copying of this information by myself or by anyone other than the intended recipient(s) is unauthorized.

Print Name Signature

Date

OCDSB Representative (Supervisory Officer / Principal / Manager / Supervisor):

Print Name Title Signature

Date