Privacy Breach Procedure: New Procedure

To: Governance and Policy Committee

Date: 27 April, 2022

Report No.: 04-22-4315

Strategic Directions

- Create a Culture for Student and Staff Well-Being
- Allocate Human and Financial Resources Strategically to Support Student Needs

Recommendation

It is recommended that the Privacy Breach Procedure, as presented in this report, be received for information.

Context

The Privacy Breach Procedure (the "Procedure") (see Appendix A) was developed to establish a consistent process for addressing confirmed or suspected privacy breaches of entrusted Personal Information under TDSB's obligations of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Education Act*. The Procedure supports implementation of the Freedom of Information and Protection of Privacy Policy (P094) as it establishes process and requirements for a prompt and well-coordinated response should a privacy breach occur. The Procedure also identifies implementation steps for preventing privacy breaches.

In developing the Procedure, staff incorporated provisions that improve TDSB information management practices, consistent with the Records and Information Management Policy (P097).

The Privacy Breach Procedure was approved by Executive Council on April 19, 2022 and is being presented to the Committee for information.

Action Plan and Associated Timeline

Subject to the Governance and Policy Committee's receipt, the Procedure will be provided to the Board of Trustees on May 25, 2022 for information.

Resource Implications

Not applicable

Communications Considerations

The Privacy Breach Procedure will be posted on the Board's internal and external website and communicated through the System Leaders' Bulletin.

Board Policy and Procedure Reference(s)

- Acceptable Use of Information Technology Resources Policy (P088)
- Equity Policy (P037)
- Freedom of Information and Protection of Privacy Policy (P094)
- Freedom of Information and Protection of Privacy Procedure (PR676)
- Records and Information Management Policy (P097)

Appendices

- Appendix A: Privacy Breach Procedure

From

Craig Snider, Interim Associate Director, Business Operations and Service Excellence at craig.snider@tdsb.on.ca

Leola Pon, Executive Officer, Legal Services at leola.pon@tdsb.on.ca

Elmira Chimirova, Senior Legal Counsel, Legal Services at elmira.chimirova@tdsb.on.ca

APPENDIX A

Toronto District School Board

Operational Procedure PR736

Title: **PRIVACY BREACH**

Adopted: **April 19, 2022**
Effected: **April 19, 2022**
Revised: N/A
Reviewed: N/A
Authorization: Executive Council

1.0 RATIONALE

The Privacy Breach Procedure (the "Procedure") supports the implementation of the Freedom of Information and Protection of Privacy Policy (P094), Freedom of Information and Protection of Privacy Procedure (PR676) and the Acceptable Use of Information Technology Resources Policy (P088).

As an accountable organization, Toronto District School Board ("TDSB") is committed to protecting the Personal Information entrusted to it and continually improving its information handling practices.

2.0 OBJECTIVE

- To establish a consistent process for addressing confirmed or suspected Privacy Breaches of entrusted Personal Information under TDSB's obligations of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Education Act*.
- To provide guidelines and requirements for designated staff to follow if a Privacy Breach occurs as defined in MFIPPA and the *Personal Health Information Protection Act* (PHIPA).
- To allow for a prompt, reasonable and coordinated response should a Privacy Breach occur.

3.0 DEFINITIONS

Employee or *Staff* is an individual employed by TDSB to perform services in exchange for a salary or an hourly wage on a casual, temporary or permanent basis, including, but not limited to, centrally assigned staff, school personnel and/or contracted staff.

FOI and Privacy Office is TDSB's Freedom of Information and Privacy Office.

Major Privacy Breach, for the purpose of this Procedure, is a type of Privacy Breach determined by the FOI and Privacy Office which by its nature and seriousness requires an immediate response and must be reported to the IPC as soon as practicable. The cause of the breach, the risks associated with the breach and any foreseeable harm from the breach will be evaluated by the FOI Office and action will be taken, if required, to mitigate any future risk.

Contract Owner refers to a designated employee with the Approval Authority (as defined in Operational Procedure PR711 (Delegation of Authority Procedure)) who approved the agreement with a third-party service provider. Examples include but are not limited to school principal, department manager, or executive officer.

Data is facts, figures and statistics objectively measured according to a standard or scale, such as frequency, volumes or occurrences and forms the basis of Information.

Five-Step Response Protocol refers to the five steps taken by the Program Area and the FOI and Privacy Office in responding to a Privacy Breach. These steps can occur simultaneously and in quick succession. Each step does not have to be completed before beginning the next step.

Information is meaning and value derived through the analysis and interpretation of Data. Information may include but is not limited to TDSB student records, employee records, confidential, personal, or professional information and communications or any other electronically formatted information.

Information Privacy Commission ("IPC") of Ontario is an independent officer of the Ontario Legislature with the powers and duties prescribed by the *Municipal Freedom of Information and Protection of Privacy Act,* and the *Personal Health Information and Protection Act.* The office of the IPC is an independent body tasked with upholding and promoting open government and the protection of personal privacy in Ontario. The Commissioner has the authority to conduct investigations, issue order, enforce fines and review disclosure decisions.

Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA") establishes legal obligations on how public organizations, including school boards, may collect, use and disclose Personal Information. MFIPPA also establishes a right of access that enables individuals to request their own Personal Information and have it corrected.

Parent/Guardian refers to a guardian or any other caregiver legally recognized as acting in place of the parent.

Personal Information (as defined in MFIPPA) is recorded information about an identifiable individual which will be treated as confidential unless it is public information or, unless the individual consents to its disclosure or, disclosure of the

information is otherwise permitted by MFIPPA. Personal information may include, but is not limited to:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- 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,
- any identifying number, symbol or other particular assigned to the individual,
- the address, telephone number, fingerprints or blood type of the individual,
- the personal opinions or views of the individual except if they relate to another individual,
- 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,
- the views or opinions of another individual about the individual, and
- 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.

Privacy is the right of interest of an individual to control the collection, use and disclosure of their Personal Information. Privacy is a fundamental right for citizens of Ontario. School boards that collect Personal Information are required to follow legal obligations outlined in *MFIPPA*.

Privacy Breach occurs when there is unauthorized access to or collection, use, disclosure, or disposal of Personal Information ("PI") or personal health information ("PHI"). Such activity is "unauthorized" if it occurs in contravention of MFIPPA or, if applicable, a relevant provision of PHIPA. Examples of such unauthorized activities or incidents include but are not limited to; loss or theft of equipment containing Personal Information (e.g., memory sticks, disks, laptops), emails sent to a wrong address or person, incorrect file attached to an email, disposal of equipment containing Personal Information without secure destruction, insufficient controls in place to protect Personal Information in paper and electronic files, information faxed to a wrong number, use of laptop, disks, memory sticks or other equipment to store or transport Personal Information outside the office without adequate security measures.

Privacy Complaint is a complaint lodged with the Information and Privacy Commissioner of Ontario against TDSB, where it is believed TDSB has compromised or breached privacy protection rights by inappropriately collection, using, disclosing or destroying Information.

Privacy Impact Assessment (PIA) is a risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology, program, process or other activity may have on an individual's privacy.

Program Area refers to related activities or services within TDSB, who are responsible and accountable for the Data in their custody. Examples include but are not limited to: Schools, Departments, and Offices.

Service Level Agreement (SLA) is a contract between a service provider and the end user (TDSB) that defines the level of service expected from the service provider. The SLA records a common understanding about services, priorities, responsibilities, guarantees and warranties.

Supervisor is a person in charge of a workplace or has authority over Staff. This includes and not limited to a School Principal, Superintendent, Centrally Assigned Principal, Coordinator, Program Manager, Department Manager, Team Leader, and Executive Officer.

Third Party Service Provider(s) refers to a company or entity with whom TDSB has an agreement to provide a product or service to TDSB.

TDSB refers to Toronto District School Board, which is also referred to as the "*Board*".

Trustees refers to a person who is a member of the Board of Trustees and includes student Trustee.

Volunteers is an individual who performs work or provides services for TDSB, without the expectation, promise, or receipt of any compensation for their work or services.

4.0 RESPONSIBILITY

Associate Director, Business Operations and Service Excellence, Executive Officer, Legal Services, and Freedom of Information ("FOI") Coordinator.

5.0 APPLICATION AND SCOPE

This Procedure applies to all Employees, Third Party Service Providers, and Volunteers. This Procedure also impacts TDSB students and their parents/guardians.

6.0 PROCEDURE

Process for Responding to Privacy Breaches

6.1 Employees and Volunteers

6.1.1 Any Employee and Volunteer who becomes aware of a possible breach of privacy involving Personal Information or personal health information in the custody or control of the TDSB will immediately inform their Supervisor, who will verify the circumstances of the breach to the extent possible and, if satisfied that a breach has or may have occurred, will contact the FOI and Privacy Office.

6.1.2 All Employees and Volunteers will:

(a) upon discovery of potential Privacy Breach, notify their Supervisor immediately, or, in their absence, FOI Coordinator upon becoming aware of a breach or suspected breach; and,

(b) contain, if possible, the suspected breach by suspending the process or activity that caused the breach.

6.1.3 When faced with a potential Privacy Breach, all Employees and Volunteers will:

(a) retrieve hard copies of any Personal Information or personal health information that has been disclosed;

(b) ensure that no copies of the Personal Information or personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required:

(c) determine whether the breach would allow unauthorized access to any other Personal Information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system).

(d) notify individuals whose privacy was breached in writing;

(e) provide details of the extent of the breach and the specifics of the Personal Information at issue;

(f) cooperate in any further investigation into the incident undertaken by the IPC;

(g) advise of the steps that have been taken to address the Privacy Breach, both immediate and long term.

6.2 Supervisor

The Supervisor will be the lead in working with the FOI and Privacy Office to complete the necessary steps to remediate the Privacy Breach. Supervisors have the ultimate responsibility to alert the FOI Coordinator of a breach or suspected breach and to work with the FOI Coordinator to implement the five steps of the privacy breach protocol as set out below.

6.2.1 On becoming aware of a potential Privacy Breach, the Supervisors have the responsibility to:

(a) obtain all available information about the nature of the Privacy Breach or suspected breach and determine what happened;

(b) identify the scope and extent of the potential breach, such as identify the number of individuals affected, the Personal Information or personal health information involved and how the Privacy Breach occurred;

(c) take the necessary steps to stop the continuance of the Privacy Breach or continued access to the Personal Information or personal health information. For example, removal of the Personal Information or personal health information that was inadvertently posted, retrieval of the Personal Information or personal health information that was sent to the wrong recipient;

(d) alert the FOI and Privacy Office and provide as much information about the Privacy Breach as is currently available;

(e) work with the FOI Coordinator to undertake all the appropriate actions to contain the Privacy Breach; and

(f) ensure that details of the Privacy Breach and corrective actions are properly documented.

6.2.2 The Data or Information that was breached must be contained in the following ways:

(a) recalled if a distribution mechanism like email was used, along with seeking confirmation of destruction of the e-mail from the individual who received the unintended e-mail;

(b) retrieved if inadvertently disclosed, posted or published;

(c) liaise with the FOI and Privacy Office to implement the five-steps response protocol;

(d) inform the Program Area senior management for example: Superintendent, Executive Officer, of the Privacy Breach;

(e) confirm that no individual or organization is in possession of unauthorized Personal Information or personal health information;

(f) contact the local police services if the Privacy Breach was a result of a criminal activity, such as break and enter or theft;

(g) issue a breach notification letter to the affected parties using the draft provided by the FOI and Privacy Office. The individual(s) will be notified if the Privacy Breach poses a risk of identity theft, credential theft, physical harm, or loss of business or potential employment opportunities; and

(h) develop a plan, make and implement the recommendations from the FOI and Privacy Office to prevent the occurrence of a similar Privacy Breach. Make recommendations for the prevention of future Privacy Breaches, such as: increasing employee training, creating additional restrictions for access to Personal Information, strengthening existing methods of protection of Personal Information, review of policies, procedures, practices, and any other remedial action.

6.2.3 The Supervisor is the key decision maker in responding to Privacy Breaches and has the responsibility to:

(a) brief senior management (e.g., Superintendent, Associate Director, Director of Education), as necessary and appropriate.

(b) review internal investigation reports and approve required remedial action;

(c) monitor implementation of remedial action; and

(d) ensure that those whose Personal Information has been compromised are informed as required.

The Director of Education, through the Executive Officer, Legal Services, may brief Trustees on Major Privacy Breaches, as necessary and appropriate.

6.3 FOI and Privacy Office

FOI and Privacy Office plays a central role in the response to a Privacy Breach by ensuring that all five steps of the response protocol are implemented. FOI and Privacy Office will investigate, validate, and ensure compliance with MFIPPA and IPC recommendations on the privacy breach response.

FOI and Privacy Office will coordinate with Supervisors to implement the **five-step response** protocol.

6.3.1 **STEP 1 - Respond/Access**

FOI and Privacy Office will:

(a) work with the school/department to assess the situation to determine if a Privacy Breach has indeed occurred;

(b) investigate and confirm whether Personal Information and/or personal health information is involved and the extent and scope of the Privacy Breach;

(c) direct to the correct Program Area if reported from outside of TDSB;

(d) validate the privacy breach response and advise the Supervisor of the gaps for remediation;

(e) provide advice on what steps to take to respond to the Privacy Breach;

(f) require the Supervisor to complete the Privacy Breach Report (Appendix A) and return it to FOI and Privacy Office as soon as possible;

(g) report the Privacy Breach to key persons within TDSB and, if necessary, law enforcement authorities;

(h) notify TDSB Legal Services, FOI Coordinator, Risk Management, and Senior Management if considered a Major Privacy Breach; and

(i) notify TDSB Cyber Security & Risk Management team (TDSB Information Technology Services), to determine whether the cyber security incident response management process needs to be invoked.

6.3.2 **STEP 2 - Contain**

Immediately upon identification of a Privacy Breach, Supervisors with the assistance of all involved in the Privacy Breach, will identify the nature and scope of the Privacy Breach and take necessary actions to contain it.

FOI and Privacy Office will:

(a) ensure the Supervisor has taken the necessary steps to contain the Privacy Breach;

(b) identify the scope of the Privacy Breach and take corrective steps to contain it.

(c) Examples of containment activities may include:

i. Retrieving and securing any records and Personal Information that may have been disclosed (in either hard copy or electronic);
ii. Revoking access temporarily, or permanently, to the affected system; revoking/changing computer access codes;
iii. Correcting weaknesses in physical or electronic security;
iv. Ensuring that no Personal Information has been retained on any unauthorized recipient;
v. Suspending the practice(s) and process(es) that resulted in the Privacy Breach or incident;
vi. Shutting down the information system that was potentially breached; and/or
vii. Any other actions necessary to contain the Privacy Breach or incident.

All containment activities or attempts to contain will be documented by the Supervisor any other individual(s) involved in containing the Privacy Breach and report back to FOI and Privacy Office.

6.3.3 **STEP 3 - Investigate**

FOI and Privacy Office will conduct an investigation into the Privacy Breach. During the investigation process, FOI and Privacy Office may request the attendance of the individuals involved in the Privacy Breach, their Supervisor and/or TDSB Cyber Security & Risk Management team (TDSB Information Technology Services) involved in the Privacy Breach at an information-gathering meeting.

FOI and Privacy Office will:

(a) once the Privacy Breach is contained, conduct an investigation with the involvement of other parties as necessary;

(b) review the events that led to the Privacy Breach;

(c) evaluate the risk of the exposure as related to the affected Personal Information;

(d) determine if the Privacy Breach was benign (e.g. human error, accidental) or malicious (e.g. deliberate sabotage, hacking);

(e) determine who was affected by the Privacy Breach and how many were affected, what types of Personal Information were involved and how sensitive it is (e.g., email address vs. personal health information);

(f) determine if the affected Personal Information could be used for fraudulent or otherwise, harmful purposes (e.g., identity theft, access to system/devices, public humiliation);

(g) identify who had unauthorized or inappropriate access to the Personal Information;

(h) evaluate the effectiveness of the containment activities;

(i) determine if any other institutions need to be contacted (e.g., Toronto Police Service, etc.);

(j) recommend remedial action, so future Privacy Breaches do not occur; and

(k) take note of any other factors relevant to the circumstances, document the results of internal investigation and chronological events of the Privacy Breach for record keeping and keep an ongoing record of events as they unfold.

6.3.4 **STEP 4 - Notify**

Notification helps to ensure affected parties can take remedial action, if necessary; and supports a relationship of trust and confidence with TDSB. The individuals whose Personal Information was disclosed should be notified immediately upon discovery of the Privacy Breach or as soon as possible thereafter. The preferred method of notification is direct – by phone, letter or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach. See Appendix B for sample letter.

Notification helps to ensure affected parties can take remedial action, if necessary, and to support a relationship of trust and confidence. Notification will involve the following considerations:

(a) the Supervisor will consult with the FOI and Privacy Office to determine what notifications are required;

(b) affected individuals will be notified by the Supervisor promptly and, depending on the nature/scope of the Privacy Breach, notification may occur in stages;

(c) method of notification will 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 (i.e.: by phone, letter, email or in person). This will depend on the circumstances (i.e. risk, exposure, sensitivity). FOI and Privacy Office will provide a draft privacy breach notification letter to the Supervisor to issue to the affected parties. The notification letter will include details and extent of the Privacy Breach and type of Data breached;

(d) individual(s) will be notified by the department associated with the Privacy Breach (e.g., student information by the Principal, employee information by TDSB Employee Services);

(e) notifying TDSB IT Services of any accounts that have to be disabled based on assessment of risk of credential theft; and

(f) notifying the IPC where appropriate. FOI and Privacy Office will play a role in

i. informing the IPC of the Privacy Breach and work together constructively with IPC staff;
ii. conducting an internal investigation into the matter, linked to the IPC's investigation. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) review the circumstances surrounding the Privacy Breach; and 3) review the adequacy of existing policies and administrative procedures in protecting Personal Information and personal health information;
iii. addressing the situation on a systemic basis if warranted.
iv. advising the IPC of your findings and work together to make any necessary changes; and
v. cooperating in any further investigation into the incident undertaken by the IPC.

Privacy Breaches involving the following factors may be reported to the IPC:

- sensitive Personal Information (e.g., financial, employment, or health information);
- a large number of affected individuals (e.g., 50 or above);
- where the Privacy Breach has proven difficult for TDSB to contain without the assistance of the IPC; or
- it is determined by TDSB that it is in the public interest to provide such a report.

(g) How to Determine If Notification to the Affected Individuals Is Required

The following factors should be considered when determining whether notification to the affected party is required:

i. <u>Personal Health Information</u>

- Does the Privacy Breach involve the theft, loss or unauthorized use or disclosure of personal health information?

ii. <u>Risk of Identify Theft</u>

- Is there a risk of identity theft or other fraud as a result of the Privacy Breach? How reasonable is the risk? Identity theft is a concern if the Privacy Breach h includes the following but is not limited to: 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 by third parties (e.g., financial).

iii. Risk of Physical or Psychological Harm

- Does 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 report cards, mental health records, medical records, or disciplinary records.

iv. Risk of Loss of Business or Potential Employment Opportunities

- Could the loss of information result in damage to an individual's reputation, affecting their business or employment opportunities?

(h) Notification should be done promptly, and will include:

- a description of potential or actual risks or harm;
- the nature of potential or actual risk or harm;
- containment steps taken;
- what mitigating actions TDSB was/is taking;
- appropriate action for individuals to take to protect themselves against harm;
- a contact person for questions or to provide further information; and
- contact information for the Information Privacy Commissioner of Ontario if the IPC is investigating. Include an explanation of the individual's right to complain to the IPC. Contact information: Information and Privacy Commissioner/Ontario, phone: 1-800-387-0073, email: info@ipc.on.ca, website: www.ipc.on.ca

6.3.5 **STEP 5 - Implement Change and Prevention**

FOI and Privacy Office will take measures or actions, as appropriate, having regard to the seriousness of the Privacy Breach and any additional risks identified when reviewing the TDSB privacy breach report. Additionally, FOI and Privacy Office will consider if further measures are required to prevent the occurrence of a similar Privacy Breach and inform appropriate Staff of any findings and/or recommended remedial action(s).

FOI and Privacy Office will complete the following steps:

(a) review the relevant information management systems to enhance compliance with privacy legislation;

(b) initiate amendment and reinforcement of existing policies, procedures, and practices for managing and safeguarding Personal Information;

(c) develop and implement new security privacy measures, such as Privacy Impact Assessment, if required with the assistance of TDSB Information Technology Services;

(d) review employee training/awareness on legislative requirements, security and privacy procedures and practices to reduce potential or future 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; and/or

(f) recommend remedial action to the Director of Education or designate, where appropriate.

(g) **Prevention.** Once the immediate steps are taken to mitigate the risks associated with the Privacy Breach, FOI and Privacy Office will further investigate the cause of the Privacy Breach as necessary. As a result of this evaluation, FOI and Privacy Office will assist the responsible Staff to put into effect adequate long-term safeguards against further breaches, such as assisting with the implementation of appropriate technical, physical or administrative safeguards designed to prevent any subsequent breach of Personal Information, arranging employee training on privacy, consider having an outside party review processes and make recommendations (e.g. auditing company), evaluating the effectiveness of remedial actions.

6.4 Third-Party Service Providers

6.4.1 All third-party service providers must take steps to ensure that all Personal Information ion and/or personal health information in their custody or to which they have access as part of their services to TDSB is protected in accordance with the requirements set out MFIPPA, TDSB's policies and procedures and are in compliance with requirements outlined in contracts or Service Level Agreements.

All third-party service providers should abide by TDSB privacy requirements, with respect to the security and privacy of Personal Information within the third-party service provider product(s). Typical third-party service providers include but are not limited to, commercial school photographers, bus companies, external data warehouse services, IT software or solution provider, online services providers, external researchers, and external consultants.
Municipal or provincial third-party entities, such as: Children's Aid Society (CAS), Public Health Units (PHU), are bound by MFIPPA.

TDSB Owned Contracts:
Contracts that are signed between third -party service providers and TDSB to provide a product or service TDSB wide. An example of a district owner contract includes but is not limited to: G Suite for Education.

Locally Owned Contracts:
Contracts that are signed between third-party service providers and a local department or school. An example of a locally owned contract includes but is not limited to, an after-school program delivered to one school by a third party.

The responsibility lies with the Contract Owner to ensure third-party service provides comply with the expectations outlined in this Procedure for new and existing contracts, Therefore, it is critical that privacy terms of the service are included in any school-based agreement, contract or Service Level Agreement.

If a school or department plans to purchase, acquire or subscribe to digital tools or resources provided by third-party service providers (e.g. purchase of software, purchase of web-based solution; subscription to remote services and tools; subscription to online applications, etc.) these types of arrangements should be vetted by TDSB IT Services through cyber risk and Privacy Impact Assessments . These Privacy Impact Assessments identify privacy risks of the proposed initiative, analyze the need for the proposed data elements to be used, describe the proposed data flows and determine compliance with the TDSB privacy laws. Third-party service providers should comply with all recommendations and protocols set out in Privacy Impact Assessments and Service Level Agreements when online resources, portals and platforms (with or without fees) are being provided to TDSB.

6.4.2 In the event a third-party service provider becomes aware of and objectively confirms the presence of any unauthorized or improper access to, use of and disclosure of any Data, including any known or suspected security breach, data loss or other adverse event known or reasonably believed to have compromised the security, integrity, availability or confidentiality of any Data in its possession or under its care and control, a third-party service providers must:

(a) notify TDSB immediately when a Privacy Breach or suspected breach is discovered and inform FOI and Privacy Office of any progress in breach investigation. A third-party service provider will provide notification to TDSB within a reasonable amount of time of confirmation of the incident, not exceeding seventy-two (72) hours;
(b) take all reasonable steps to mitigate any harmful effect resulting from any such unauthorized access to, use or disclosure of Data;
(c) adhere to steps set out in section 6.2.1 of this Procedure;
(d) adhere to the recommendations set out in the Privacy Impact Assessments;
(e) fulfill all contractual or Service Level Agreement obligations to comply with the TDSB privacy requirements;
(f) adhere to all applicable TDSB privacy laws and all TDSB requirements with respect to a Privacy Breach related to Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation, where commercially reasonable, of any such Privacy Breach; and
(g) must have a written incident response plan that reflects best practices and is consistent with industry standards and federal and provincial law and any other

applicable law, for responding to a Privacy Breach, breach of security, privacy incident, or unauthorized acquisition or use of Data or any portion thereof, including Personal Information and agrees to provide TDSB, upon request, with a copy of said written incident response plan

6.4.3 In the event of a Privacy Breach, a third-party service provider will follow the following process regarding the provision of the privacy breach notification:

(a) the security breach notification will be written in plain language, will be titled "Notice of Privacy Breach", and will present the information described herein under the following headings: "What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do", and "For More Information". Additional information may be provided as a supplement to the notice.
(b) the security breach notification described above in section 6.4.3(a) will include, at a minimum, the following information:
    i. the name and contact information of TDSB's designee or his/her designee for this purpose.
    ii. a list of the types of Data that were or are reasonably believed to have been the subject of a Privacy Breach.
    iii. if the information is possible to determine at the time the notice is provided, then either (1) the date of the Privacy Breach, (2) the estimated date of the Privacy Breach, or (3) the date range within which the Privacy Breach occurred. The notification will also include the date of the notice.
    iv. whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
    v. a general description of the privacy breach incident, if that information is possible to determine at the time the notice is provided.

A third-party service provider will reasonably co-operate and assist in, any investigation of a complaint that any Data has been collected, used or disclosed contrary to the TDSB privacy laws, or the policies and procedures of TDSB, whether such investigation is conducted by TDSB itself or a body having the legal authority to conduct the investigation, including but not limited to co-operation and assistance in notifying the affected individual(s) of the unauthorized access, which will include the information listed in this section.

6.4.4 If a third-party service provider receives a request for access to any Personal Information from any person (other than TDSB), a third-party service provider will promptly advise a requester to make the request to TDSB and, if TDSB has advised a third-party service provider of the name or title and contact information of a specific official of TDSB to whom such requests are to be made, TDSB will also promptly provide that official's name or title and contact information to the requestor.

6.5 Non-Compliance

Non-compliance with this Procedure places TDSB in a potential legal liability scenario. Privacy breaches may cause irreparable harm to individuals to whom TDSB owes a duty of confidence, and that the injury and harm to those individuals may be difficult to calculate and inadequately compensable in damages.

7.0 EVALUATION

This Procedure will be reviewed and updated as required, but at a minimum every four (4) years after the effective date.

8.0 APPENDICES

Appendix A: Privacy Breach Report
Appendix B: Sample Notification Letter

9.0 REFERENCE DOCUMENTS

Policies:

- Freedom of Information and Protection of Privacy Policy (P094)
- Acceptable Use of Information Technology Resources Policy (P088)
- Policy - Records and Information Management (P097)
- Procedure - Records and Information Management (PR677)

Procedures:

- Procedure - Cyber Risk and Security (PR725)
- Procedure - Police-School Board Protocol (PR698)
- Freedom of Information and Protection of Privacy (PR676)

Legislative Acts and Regulations

- *Education Act, R.S.O. 1990, c. E.2*
- *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56*
- *Personal Health Information Protection Act, 2004,* SO 2004, c.3 Sched. A
- Ontario Student Record Guidelines

Other

- IPC: Privacy Breaches: *Guidelines for Public Sector Organizations*
- IPC: Breach Notification Assessment Tool, December 2006
- IPC: What to do if a Privacy Breach Occurs: Guidelines for Government Organizations, May 2003

- IPC: Planning for Success: Privacy Impact Assessment Guide
- IPC: Thinking About Clouds? Privacy, Security, and Compliance Considerations for Ontario Public Sector institutions
- IPC: Open Government and Protecting Privacy
- IPC: Fact Sheet, Video Surveillance

APPENDIX A

APPENDIX A

TDSB Privacy Breach Report
(Operational Procedure PR736)

TDSB File Reference # *(assigned by FOI and Privacy Office):*
_____

IPC File Reference # *(if applicable):*
_____

To be completed by the Supervisor.

Please use this report as a guide to provide FOI and Privacy Office with as much information as possible about the incident in question.

Take immediate action when you have been advised of a suspected privacy breach. Many of the steps outlined below have to be carried out simultaneously or in quick succession. Steps 1 and 2 are completed based on the information received either directly from an employee, or orally through his/her immediate supervisor (e.g., phone call), or in written form (e.g., email).

The following steps are to be initiated as soon as a privacy breach or suspected breach has been reported.

STEP 1 - RESPOND

1. Person Reporting Suspected Breach:

Date: _____

First name: _____

Last name: _____

Job title: _____

Location (school/department): _____

Learning Centre (if applicable): _____

Name of immediate supervisor: _____

Phone number: _____

_____

Email: _____

2. When Incident Occurred:

Date - _____ **Time** - _____
(mm/dd/yyyy) (a.m. or p.m.)

3. Contact:

Internal Source – (Identify) _____

External Source – (Identify) _____

4. Identify steps taken to respond to privacy breach:

_____

_____

_____

_____

_____

_____

STEP 2 - CONTAIN

5. Describe what happened:

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
- ☐ theft of Personal Information
- ☐ other – please explain:

_____

_____

6. **Describe the background and scope of the Privacy Breach. Describe how the Privacy Breach happened, including a chronology of events:**

7. **Indicate the date of incident or range:**

8. **Indicate the date on which the incident discovered and how:**

9. **Indicate the date when the Privacy Breach was reported to the supervisor and who reported the Privacy Breach:**

10. **Indicate the location of the incident:**

11. Describe the containment activities and efforts (e.g., suspending the process/activity that caused the Privacy Breach):

12. Describe the immediate steps taken to reduce the harm of the Privacy Breach (e.g. locks changed, computer access codes changed, shredding hard copies, recalling of emails, double deleting emails, return of the records back to TDSB, etc.):

STEP 3 - INVESTIGATE

13. Identify the events that led to the Privacy Breach:

14. Source and cause of the Privacy Breach. What was the cause of the breach (for example: human error, technical error, phishing email, ransomware, cyber-attack, other?)

15. **Provide an estimated number of individuals affected by the incident:**

16. **Describe the Personal Information involved (e.g. first and last name, address, phone numbers, Student Numbers, Employee Number, financial (Social Insurance Number, Credit Card Information, bank accounts, etc.), medical (Health Card Numbers, sensitive medical information, etc.)):**

17. **To whom the Personal Information belongs to (e.g., student, employee, third party [someone who is neither a student nor employee of the board, such as a parent/guardian or volunteer]):**

18. **Who had unauthorized access to the Personal Information, and how that access was made?**

19. **Describe physical security measures that are in place (e.g. alarms, locks on the cabinets and doors):**

20. **Describe technical measures that are in place (e.g. Encryption, password protection, other):**

STEP 4 – NOTIFY

If a breach HAS occurred refer to “How to Determine if Notification is Required” in the Procedure.

21. **What date was the Freedom of Information and Privacy Office notified:**

22. **Was TDSB IT Services/Cybersecurity team notified? And when? What is the incident number (if applicable)?**

23. **Have the law enforcement agency or other authorities been notified and when. Provide a copy of an incident report and/or report number:**

24. Have you contacted/notified the affected parties or individuals whose privacy was compromised?

Notify the following individuals as appropriate:

- ☐ Individuals whose privacy was breached.

Provide them with information about:

- what happened;
- the nature of potential or actual risks or harm;
- what mitigating actions the board is taking;
- appropriate action for individuals to take to protect themselves against harm; and
- 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 IPC about TDSB's handling of their Personal Information, along with contact information for IPC.

- ☐ Director of Education
- ☐ Senior administration/managers/principals
- ☐ Legal Counsel
- ☐ Information and Privacy Commissioner/Ontario ("IPC")
- ☐ Other

STEP 5 – IMPLEMENT CHANGE AND PREVENTION

25. Describe the long-term strategies you will take to correct the situation (e.g. staff training, security protocols, policy development, contractor supervision, improved physical security, improved technical security):

26. Propose steps that need to be taken to prevent future breaches (e.g. ensure strengthening of security and privacy controls, recommend appropriate and

necessary security safeguards, arrange employee training on privacy and security, change or enhance policies and procedures, etc.):

_____

_____

_____

_____

_____

_____

27. Any additional information not captured above? Please provide details:

_____

_____

_____

_____

_____

_____

Received by FOI and Privacy (Date): _____

Following a report of a suspected Privacy Breach, ensure that the activity/process has been contained if possible. Conduct an investigation of the information supplied in Steps 1 and 2 of this report in conjunction with current privacy legislation (MFIPPA, PHIPA) and with TDSB and local privacy policies and procedures to determine if the incident is, in fact, a breach.

APPENDIX A

APPENDIX B

SAMPLE NOTIFICATION LETTER

[Print on school or TDSB Letterhead]
[Date]
[Name of person being notified]
[Address]

Dear [Parent(s)/Guardian(s) or Name of employee]:

The protection of privacy and personal information for staff and students and diligence to our obligations under the *Municipal Freedom of Information and Protection of Privacy Act* is an ongoing priority for Toronto District School Board ("TDSB"). At this time, we are advising you of an incident …

[*Details of incident, list risks, information exposed, steps to mitigate*]

Example:
On or about [insert date], the school administration [*or Toronto District School Board ("TDSB") staff*] became aware that a school staff member [or TDSB staff member] inadvertently sent an [*describe what was sent*]. The [*email, etc*.] contained your child's [*describe what personal information the email contained*]

As part of our protocol, we have also reported the incident to the Information and Privacy Commissioner of Ontario ("IPC") to ensure that we are complying with appropriate obligations with respect to this incident. If you wish to file a complaint with the IPC the website is http://www.ipc.on.ca.

Thank you for your understanding as TDSB works through and learns from this incident. If you have any additional questions, you are welcome to contact the undersigned.

Sincerely,

[Signature of Principal or Supervisor/Manager]