**PR736A**

**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: |  |

1. **When Incident Occurred:**

**Date -** \_\_\_\_\_\_\_\_\_\_\_ **Time** - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(mm/dd/yyyy) (a.m. or p.m.)

1. **Contact:**

Internal Source – (Identify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

External Source – (Identify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Identify steps taken to respond to privacy breach:**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**STEP 2 - CONTAIN**

1. **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:

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

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

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |
|  |
|  |
|  |

1. **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**

1. **Identify the events that led to the Privacy Breach:**

|  |
| --- |
|  |
|  |
|  |

1. **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?)**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

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

|  |
| --- |
|  |

1. **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.)):**

|  |
| --- |
|  |
|  |
|  |

1. **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]):**

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

1. **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.

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |
|  |
|  |

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

|  |
| --- |
|  |
|  |

1. **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**

1. **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):**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

1. **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.):**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

1. **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.