Procedures for Responding to Privacy Critical Incidents and Breaches

Link to Parent Policy:	*Privacy Policy*		
Procedure Reference:	PRPR01_2211N_AD/PRE		
Procedure Sponsor:	President		
Procedure Contact:	Privacy Officer		
Stakeholders:	All members of the OC Community including: Employees, Students, and the Board of Governors		
Approved by:	Executive Team		
Effective Date:	March 22, 2023		
Last reviewed:	December 2022	Scheduled review date:	December 2027

1. Purpose

Okanagan College is committed to ensuring the protection and security of all personal information within its control. That commitment includes responding effectively and efficiently to privacy breach incidents that may occur.

The purpose of this Procedure is to set out Okanagan College's process for responding to significant critical incidents and privacy breaches such as the theft or loss of or the collection, use or disclosure of Personal Information not authorized by FIPPA, and includes cyber attacks and other situations where there are reasonable grounds to believe that any such unauthorized activities have taken place or there is a reasonable belief that they will take place. The College is committed to complying with the notice and other obligations under the *Freedom of Information and Protection* of *Privacy Act* (FIPPA).

2. Scope & Responsibility

All Employees of the Okanagan College are expected to be aware of and follow this Procedure in the event of a privacy breach. This Procedure applies to all Employees, contractors and volunteers of the College.

3. Responsibilities of Employees

3.1 All Employees must without delay report all actual, suspected or expected Privacy Breach incidents of which they become aware in accordance with this Procedure. All Employees have a legal responsibility under FIPPA to report Privacy Breaches.

3.2 Privacy Breach reports should be made to the Privacy Officer at *privacy@okanagan.bc.ca*, who has delegated responsibility for receiving and responding to such reports.

3.3 The Privacy Officer will promptly inform the Head of any Privacy Breach Report received.

3.4 If there is any question about whether an incident constitutes a Privacy Breach or whether the incident has occurred, Employees should consult with the Privacy Officer.

3.5 All Employees must provide their full cooperation in any investigation or response to a Privacy Breach incident and comply with this Procedure for responding to Privacy Breach incidents.

3.6 Any Employee who knowingly refuses or neglects to report a Privacy Breach in accordance with this Procedure may be subject to discipline, up to and including dismissal.

4. Privacy Breach Response

Step One – Report and Contain

4.1 Upon discovering or learning of a Privacy Breach, all Employees shall:

a) Immediately report the Privacy Breach to the Privacy Officer.

b) Take any immediately available actions to stop or contain the Privacy Breach, such as by:

c) isolating or suspending the activity that led to the breach; and

d) taking steps to recover Personal Information, Records or affected equipment.

e) preserve any information or evidence related to the Privacy Breach to support the College's incident response.

4.2 Upon being notified of a Breach Incident the Privacy Officer in consultation with the Head, shall implement all available measures to stop or contain the Breach Incident. Containing the Breach Incident shall be the priority of the Breach Incident response, and all Employees are expected to provide their full cooperation with such initiatives.

Step Two – Assessment and Containment

4.3 The Privacy Officer shall take steps to contain the Breach Incident by making the following assessments:

a) Identifying the cause of the Breach Incident;

b) if any additional steps are required to contain the Privacy Breach, and, if so, to implement such steps as necessary;

c) identify the type and sensitivity of the Personal Information involved in the breach, and any steps that have been taken or can be taken to minimize the harm arising from the breach;

d) identify the individuals affected by the breach, or whose Personal Information may have been involved in the breach;

e) determine or estimate the number of affected individuals and compile a list of such individuals, if possible; and

f) make preliminary assessments of the types of harm that may flow from the Privacy Breach.

4.4 The Head, in consultation with the Privacy Officer, shall be responsible to, without delay, assess whether the Privacy Breach could reasonably be expected to result in significant harm to individuals. That determination shall be made with consideration of the following categories of harm or potential harm:

a) bodily harm;

b) humiliation;

c) damage to reputation or relationships;

d) loss of employment, business or professional opportunities;

e) financial loss;

f) negative impact on credit record,

g) damage to, or loss of, property,

h) the sensitivity of the Personal Information involved in the Privacy Breach; and

i) the risk of identity theft.

Step Three – Remediation and Notification

4.5 If the Head determines there are further actions that could be taken to reduce impact they may take those steps or direct the Privacy Officer to do so.

4.6 If the Head determines that the Privacy Breach could reasonably be expected to result in significant harm to individuals, then the Head shall make arrangements to:

a) report the Breach Incident to the Office of the Information and Privacy Commissioner; and

b) provide notice of the Breach Incident to affected individuals, unless providing such notice could reasonably be expected to result in grave or immediate harm to an individual's safety or physical or mental health or threaten another individual's safety or physical or mental health.

4.7 If the Head determines that the Privacy Breach does not give rise to a reasonable expectation of significant harm, then the Head may still proceed with arranging the notification to affected individuals if the Head determines that notification would be in the public interest or if a failure to notify would be inconsistent with the College's obligations or undermine public confidence in the College.

4.8 Determinations about notification of a Privacy Breach shall be made without delay following the Breach Incident, and notification shall be undertaken as soon as reasonably possible. If any law enforcement agencies are involved in the Privacy Breach incident, then notification may also be undertaken in consultation with such agencies.

Step 4 - Prevention

4.9 The Head, or the Privacy Officer in consultation with the Head, shall complete an investigation into the causes of each Privacy Breach reported under this Procedure, and shall implement measures to prevent recurrences of similar incidents.

5. Contact Information

Questions or comments about this Procedure may be addressed to the Privacy Officer at *privacy@okanagan.bc.ca*.

6. Related Acts and Regulations

College and Institute Act
Freedom of Information and Protection of Privacy Act (FIPPA)

7. Supporting References, Policies, Procedures and Forms

Procedures for Responding to Privacy Critical Incidents and Breaches
Procedures for Responding to Freedom of Information Access Requests
Procedures for Privacy Impact Assessments
Procedures for Website Privacy

History / Revisions

Date	Action
2022-11-09	New Procedure approved by OC Executive Team: *Responding to Privacy Critical Incidents and Breaches*