



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Calgary French & International School (Organization)
Decision number (file number)	P2019-ND-083 (File #011931)
Date notice received by OIPC	February 4, 2019
Date Organization last provided information	May 31, 2019
Date of decision	June 24, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• gender ID,• date of birth, and• primary, secondary and tertiary telephone numbers. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On November 20, 2018, a staff member accessed a report containing personal information on the Hour Zero’s school emergency program website.• The Hour Zero program automatically sent an email to all staff notifying them that their personal information had been viewed.

	<ul style="list-style-type: none"> • The incident was discovered on November 20, 2018 when the Organization’s Privacy Officer received an email alert from Hour Zero. • The Hour Zero program has a pop-up that reads, “You are about to view all staff members of this site’s confidential information. If you continue, the staff members will be notified that you have viewed their information. Do you still want to view the information?” “Ok” or “Cancel”.
Affected individuals	The incident affected approximately 120 residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Hour Zero is working on restricting access to particular reports/fields. • Asked Hour Zero to delete birth dates as the information is not required on the platform. • Notified all staff of this course of action.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on November 21, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be “significant.” It must be important, meaningful, and with non-trivial consequences or effects.</p>	<p>The Organization reported that “The type of harm is felt to be embarrassment that a personal birth date had been viewed by another staff member”. And “...a birthdate can be part of an information trawl to steal identity”.</p> <p>In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the harms of identity theft and fraud, and to make unsolicited telephone calls and/or texts. Due to personal/professional relationships between co-workers, date of birth could be used to cause the harm of humiliation or embarrassment. Identity theft, fraud, and humiliation/embarrassment are significant harms.</p>
<p>Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.</p>	<p>The Organization reported that “There is no evidence of malicious [sic] intent, rather an ignorance of taking the time to read the content of the pop-up message”. Further, “In this instance, it is felt this was more a negligent action rather than a malicious one.”</p> <p>In my view, the likelihood of significant harm resulting from this incident is decreased as the incident did not result from malicious intent, but rather human error. Identity theft and fraud are unlikely given the circumstances and considering that the individual who accessed the information is known to the Organization. The Organization provided assurances that the information was only viewed very briefly and the employee did not use, make copies, further disclose or otherwise distribute the personal information at</p>

	issue. Nonetheless, given the personal/professional relationships, humiliation and embarrassment are real risks.
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.</p> <p>A reasonable person would consider that the contact and identity information at issue could be used to cause the harms of identity theft and fraud, and to make unsolicited telephone calls and/or texts. Due to personal/professional relationships between co-workers, date of birth could be used to cause the harm of humiliation or embarrassment. Identity theft, fraud, and humiliation/embarrassment are significant harms.</p> <p>The likelihood of significant harm resulting from this incident is decreased as the incident did not result from malicious intent, but rather human error. Identity theft and fraud are unlikely given the circumstances and considering that the individual who accessed the information is known to the Organization. The Organization provided assurances that the information was only viewed very briefly and the employee did not use, make copies, further disclose or otherwise distribute the personal information at issue. Nonetheless, given the personal/professional relationships, humiliation and embarrassment are real risks.</p> <p>The Organization is required to notify the affected individuals pursuant to section 37.1 of PIPA. I understand affected individuals were notified of the incident by email on November 21, 2018. The Organization is not required to notify affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner