



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	King Edward Child Care Society (Organization)
<b>Decision number (file number)</b>	P2022-ND-082 (File #023180)
<b>Date notice received by OIPC</b>	August 8, 2021
<b>Date Organization last provided information</b>	October 6, 2022
<b>Date of decision</b>	January 17, 2023
<b>Summary of decision</b>	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	<p>The Organization is incorporated under Alberta’s <i>Societies Act</i> and qualifies as a “non-profit organization” for purposes of PIPA.</p> <p>Section 56(3) limits the application of PIPA to personal information collected, used or disclosed by a non-profit organization in connection with a commercial activity.</p> <p>Section 56(1)(a) of PIPA defines “commercial activity” to include any transaction, act, conduct, or regular course of conduct that is of a commercial character.</p> <p>In this case, the Organization delivers child care for a fee. In my view, this activity qualifies as a commercial activity. Therefore, PIPA applies to personal information at issue.</p>
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved some or all of the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• home address,</li><li>• contact information,</li><li>• police clearances, and</li><li>• certifications.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>

<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"> <li>• On July 27, 2021, a previous staff member came into the Organization’s office to return the filing cabinet key.</li> <li>• While there, the previous staff member unlocked the filing cabinet which contains staff files and took their file, along with the files of two other staff members who they hired, despite being told to leave the files in the cabinet.</li> <li>• The Organization reported that the files were returned to the Organization after the Privacy Breach Form was provided to this office.</li> </ul>
<b>Affected individuals</b>	The incident affected approximately 3 individuals.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Requested that the files be returned.</li> <li>• Retrieved the files.</li> <li>• Looking to move everything digital.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	<p>The Organization notified one employee by email and one employee verbally. However, the notifications were not in compliance with section 19.1 of the PIPA Regulations.</p> <p>The Organization reported it did not have contact information for the third individual.</p>
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<b>Harm</b> 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>The Organization reported the possible harms that may occur as a result of the breach is “Identity theft”.</p> <p>In my view, a reasonable person would consider that the contact and human resources information (police clearances and certifications) at issue could be used to cause the harms of identity theft and fraud. If email addresses forms part of the contact information, email addresses could be used for the purposes of phishing, increasing the affected individuals’ vulnerability to identity theft and fraud. Police clearance information could be used to cause humiliation or embarrassment. These are all significant harms.</p>
<b>Real Risk</b> The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship	<p>The Organization reported,</p> <p style="text-align: center;"><i>The individual who took the files, knows the other people who (sic) files were also taken. I dont (sic) think it will likely result in any harm, but the licensing privacy office told me I was mandated to report the files being taken.</i></p>

between the incident and the possible harm.

In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the actions of a third party (deliberate removal of files from the Organization). It is not clear why the staff members took the files. While the Organization did retrieve the files, it also reported that they did not get an agreement or statutory declaration from the individual who took the files that the information was not copied or re-distributed in any way. Further, the information may have been exposed for approximately two weeks.

**DECISION UNDER SECTION 37.1(1) OF PIPA**

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.

Contact and human resources information (police clearances and certifications) at issue could be used to cause the harms of identity theft and fraud. If email addresses forms part of the contact information, email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Police clearance information could be used to cause humiliation or embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the actions of a third party (deliberate removal of files from the Organization). It is not clear why the staff members took the files. While the Organization did retrieve the files, it also reported that they did not get an agreement or statutory declaration from the individual who took the files that the information was not copied or re-distributed in any way. Further, the information may have been exposed for approximately two weeks.

I understand the Organization notified two of the affected individuals by email and by phone call. However, these notifications were not in accordance with the PIPA Regulation.

**For those affected individuals where the Organization has contact information, I require the Organization to report to my office within ten (10) days of the date of this decision, that it has notified these individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation (Regulation)*.**

The Organization also reported that direct notification would not be possible for one of the affected individuals because the Organization did not have contact information.

**I require the Organization to report to my office within ten (10) days of the date of this decision, with a submission describing the Organization's reasonable attempts to find the individual's contact information and to inform me of any attempts made.**

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must ...be given directly to the individual". However, pursuant to section 19.1 (2), "...where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual

indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.” The Organization may want to consider a submission regarding indirect notification for the affected individual without direct contact information.

Cara-Lynn Stelmack  
Assistant Commissioner, Operations and Compliance