



**PERSONAL INFORMATION PROTECTION ACT  
Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	The Alberta Teachers' Association (Organization)
<b>Decision number (file number)</b>	P2021-ND-298 (File #020514)
<b>Date notice received by OIPC</b>	April 7, 2021
<b>Date Organization last provided information</b>	April 7, 2021
<b>Date of decision</b>	March 2, 2022
<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 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>	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA "personal information"</b>	<p>The incident involved the following information:</p> <ul style="list-style-type: none"><li>• name,</li><li>• school or home address,</li><li>• school or home telephone number,</li><li>• school or personal email address, and</li><li>• name of course or event for which funding support was sought.</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 type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• On September 1, 2019, online applications for professional development scholarships and bursaries were inadvertently stored in a section of the Organization's website that was accessible publicly. As a result, applicants' contact information was returned as part of search-engine results when specific searches were conducted for the contact information data fields forming part of the application form.</li></ul>

	<ul style="list-style-type: none"> <li>• The breach was discovered on April 5, 2021, when a member of the Organization searched for her own email address and Google returned the online application form they submitted for the 2019-2020 scholarship / bursary funding. The member notified the Organization via email.</li> <li>• The Organization investigated and found four other scholarship / bursary SharePoint archives were on a default setting that make them visible to the public. The Organization removed the information.</li> <li>• The Organization reported, “The information was not hacked but was returnable on a sufficiently specific Google search. There is no indication that the information was improperly accessed.”</li> </ul>
<b>Affected individuals</b>	The incident affected 1,154 individuals.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Removed the data.</li> <li>• Requested Google remove any cached versions.</li> <li>• Implemented new policy for storage of online scholarship / bursary application data.</li> <li>• Completed an audit of digital holdings in conjunction with an independent third-party service provider.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by email and followed by mail on April 7, 2021.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<p><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>	<p>The Organization reported the possible harms that might result from the incident were “Uninvited contact by third parties; professional development activities disclosed.”</p> <p>In my view, a reasonable person would consider that contact information along with funding support information could be used to cause hurt, humiliation and embarrassment, particularly if there are personal or professional relationships involved. Email addresses could be used for the purposes of phishing, increasing the affected individuals’ vulnerability to fraud. These are significant harms.</p>
<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 between the incident and the possible harm.</p>	<p>The Organization reported that it...</p> <p><i>... understands the risk of harm to be unlikely but possible. The data was returned as a search result only through an extremely targeted (sic) search (in the case of the reporting member, it resulted only through a search of her own email address as a search (sic) string). Nevertheless, the [Organization] has no way of knowing the importance individual members place on these</i></p>

	<p><i>data fields. We are therefore informing all involved in order to maintain transparency with our members.</i></p> <p>In my view, a reasonable person would consider that the likelihood of harm is reduced because the incident resulted from human error and not malicious intent. However, the Organization cannot confirm the information that was made publicly available was not accessed by unauthorized parties. Further, it appears the information may have been exposed for approximately a year and a half.</p>
--	---

**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.

A reasonable person would consider that contact information along with funding support information could be used to cause hurt, humiliation and embarrassment, particularly if there are personal or professional relationships involved. Email addresses could be used for the purposes of phishing, increasing the affected individuals’ vulnerability to fraud. These are significant harms.

The likelihood of harm is reduced because the incident resulted from human error and not malicious intent. However, the Organization cannot confirm the information that was made publicly available was not accessed by unauthorized parties. Further, it appears the information may have been exposed for approximately a year and a half.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by email and mail on April 7, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton  
Information and Privacy Commissioner