



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

News Release

**For Immediate Release
January 28, 2016**

Ministry of Education failed to protect personal information involving missing portable hard drive

VICTORIA—In an investigation report released today, B.C. Information and Privacy Commissioner Elizabeth Denham found that the Ministry of Education failed to protect the personal information of 3.4 million B.C. and Yukon students stored on a portable hard drive.

“This investigation is unique in that we are looking at events that happened more than four years ago. The passage of time and the lack of proper documentation made it difficult to gather consistent and complete information from those involved. Therefore, the main goal of this report is to highlight lessons from the past to help prevent future breaches,” said Commissioner Denham.

The Commissioner initiated an investigation in September 2015 after the Ministry of Education notified her that it was unable to locate a portable hard drive containing personal information collected between 1986 and 2009, including name, gender, date of birth and Personal Education Number.

A number of the records contained more sensitive personal information, including address, type of schooling, grade information, teacher retirement plans, education outcomes for cancer survivors, health and behaviour issues, and children in care.

The ministry used the portable hard drive as a backup for the purpose of disaster recovery of ministry research data. The information was moved from a secure server to the hard drive in an attempt to decrease electronic storage costs, and was ultimately sent to an off-site warehouse for storage.

The ministry declared the hard drive to be lost when employees were unable to locate it in the warehouse after a series of extensive searches.

The investigation found that despite having privacy and security policies in place, the ministry contravened section 30 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) when it failed to protect the personal information of millions of children and teachers after copying the information onto the portable hard drive. The ministry did not ensure the information was encrypted, did not store the portable hard drive in an approved off-site warehouse and did not adequately document the contents or location of the portable hard drive.

Once the ministry discovered the breach, its response did comply with s. 30 of FIPPA, in that its containment efforts, analysis of the risks to the affected individuals and preventative measures were appropriate.

“There are many important lessons to be learned from this investigation, not only for the Ministry of Education, but for other public agencies as well. This is an example of a breach that was completely preventable. If the ministry had implemented any one of a number of safeguards and followed existing policy, the breach would not have happened.

“This is where executive leadership has an opportunity to reinforce a multi-faceted approach to security. Measures such as maintaining a thorough personal information bank inventory, securing personal information properly and designating an appropriate retention period for records will go a long way in building a sound privacy management program.

“I am pleased to see that the ministry has already taken steps to reduce the risk of future breaches, including implementing a privacy management program and appointing a Ministry Privacy Officer.” said Denham.

Commissioner Denham has made nine recommendations to strengthen the security of personal information maintained by the ministry. The recommendations focus on steps the ministry should take to ensure policies and procedures are followed, including maintaining an accurate inventory of personal information assets, encrypting all mobile data storage devices and storing them only in government approved facilities.

In addition, mandatory training, privacy and security audits and executive leadership are critical to ensuring employees build privacy into their operations and programs.

The Commissioner’s office will follow up with the ministry in three months with respect to the implementation of these recommendations.

Investigation Report F16-01: Ministry of Education is available at:

www.oipc.bc.ca/report/investigation-reports/

Michelle Mitchell
Office of the Information and Privacy Commissioner for B.C.
250 217-7872
mmitchell@oipc.bc.ca
Twitter @BCInfoPrivacy