
FREQUENTLY ASKED QUESTIONS

Sept. 22, 2015

Ministry of Technology, Innovation and Citizens'
Services

EDUCATION DATA SECURITY BREACH

B.C.'s Ministry of Education has been unable to locate an unencrypted external hard drive that contains a variety of reports, databases, and information. Some of the files on the hard drive include personal information, such as names, gender, postal codes, grades, and in some cases addresses.

The hard drive does not contain social insurance numbers, personal health numbers, driver's licence or banking information. While there is no evidence at this time to suggest that the information has been accessed or misused in any way, government is alerting the public out of an abundance of caution because the hard drive has not been located.

With a potential data breach of this nature, there is a risk of identity theft or fraud, however that risk is considered to be low.

The Government of B.C. takes the privacy of people seriously and the Office of the Chief Information Officer (OCIO) is conducting a thorough investigation of the incident. In addition, the OCIO will be doing a cross-government review of ministry practices around the storage of personal information management.

The Information and Privacy Commissioner is also investigating this matter.

Who is affected by this potential privacy breach?

Anyone who went to an elementary, secondary or post-secondary school in B. C. or Yukon from 1986 – 2009 could have personal records on the missing hard drive.

How did the potential privacy breach happen?

The Office of the Chief Information Officer is investigating how the hard drive was misplaced. The Office of the Privacy Commissioner was also notified about the incident and has initiated a formal investigation.

What records are on the missing drive?

The personal information on the hard drive is from 1986 – 2009, and includes student's Personal Education Numbers along with some of the following information:

- Academic achievement scores from the Foundation Skills Assessment and Grade 10, 11 and 12 exam marks.
- Grade point average, graduation status.
- Those identified as Aboriginal or special needs.
- Year of birth and home postal code.

Another file includes Personal Education Numbers, names and home addresses.

- Another data set includes Personal Education Numbers flagged as cancer survivors, being studied to see how the disease affected their education records.

- It also includes files related to the Student Transitions Project which assigns all students in secondary and post-secondary institutions with a Personal Education Number.
- This information is used to track trends in student achievement and evaluate effectiveness of programs, to support researchers through formal research agreements, and for post-secondary enrollment.

A full description of data on the disc is available here:

http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/reports/Education_Data_Breach.pdf

How can I find out if I have been affected by this potential privacy breach?

- People can contact the Service BC call centre to find out if their personal was stored on the missing hard drive, based on when you or their children attended a K-12 school or a post-secondary institution in B.C. and the Yukon.
- Call centre staff will be able to tell you what type of data (name, postal code, etc.) could be on the missing hard drive, as well as any privacy steps you could take.
- People can call: **1-800-663-7867** from 7:30 a.m. - 5 p.m. Monday to Friday.
 - In Vancouver: 604-660-2421
 - In Victoria: 250-387-6121
 - In Yukon: dial 0 and ask to place a collect call to 604 660-2421
 - http://www.servicebc.gov.bc.ca/about_servicebc/

Am I at risk of identity fraud and if so, what can I do to protect myself?

While this privacy breach did not include banking information, personal health numbers, driver's licence or social insurance numbers, enough information may have been accessed to put you at risk of potential identity theft, although that risk is considered to be low.

You are encouraged to keep a close eye on your bank accounts, credit card statements, online identity and other related services. Online or mobile banking is an easy way to monitor your financial information daily; you can sign up for free with your financial institutions.

If you suspect your personal information has been put at risk you are encouraged to call Canada's national credit agencies.

- Equifax: 1 800 465-7166, press option 3 for fraud
- TransUnion: 1 800 663-9980

If you have proof that your identity has been stolen, you should call the police.

Frequently Asked Questions about Potential Identity Theft:

http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/IDtheftFAQ.pdf

Media
Inquiry
Contact:

Government Communications and
Public Engagement
250 889-1121