Craib, Patrick MTIC:EX

From: Byng, Dave A EDUC:EX
Sent: Tuesday, September 22, 2015 11:18 AM
To: EDUC DL Ministry All
Subject: Update on Potential Data Breach

To All Staff,

As you may be aware, we have been conducting a comprehensive search for an unencrypted external hard drive containing student level data. I wish to thank everyone who participated in the extensive physical search of the ministry's Victoria facilities, as well as acknowledge the countless staff who spent time away from their family and friends this past weekend to help complete a detailed analysis of the content on the drive.

While there is no evidence to suggest that the information has been improperly accessed or misused in any way, out of an abundance of caution, government is informing the public today that the hard drive has not yet been located.

Please refer to this news release and backgrounder for more information.
http://www2.news.gov.bc.ca/news_releases_2013-2017/2015MTICS0026-001575.htm

In these times, we are all reminded how important it is to protect government's information assets. As public servants, each of us is responsible for understanding our roles and responsibilities with respect to data protection and government's core polices. I recognize that the majority of staff have already completed the course titled "**Privacy and Information Sharing: Awareness Training**"; for those of you who may not have completed this course already, please complete this mandatory training (steps for registering are appended to this note).

If you are contacted by our partners in the sector, the public or media with questions about this incident, please be reminded of the following protocols:

- All questions from the public or sector partners are to be directed to the Service BC's Contact Centre at:
  - Victoria: 250-387-6121
  - Vancouver: 604-660-2421
  - Elsewhere in B.C.: 1-800-663-7867
- If for any reason media contact staff, please direct them to the Government Communications and Public Engagement office at 250-356-5963.

On behalf of our executive team, I want to once again acknowledge and thank the many staff who supported the analysis over the weekend.

Please do not hesitate to direct any questions you may have to your immediate supervisor, or any member of the executive team.

Sincerely,

Dave Byng
Deputy Minister

MISSING HARD DRIVE
KEY MESSAGES
Confidential

Sept. 22, 2015

Government takes the management of information and the protection of privacy very seriously.

That's why, out of an abundance of caution, we are notifying the public of a potential data breach.

We are not aware of any access to, or use of, the data. Based on the type of data, the risk of identity theft is low.

Individuals can call Service BC to find out if their personal data was on the missing hard drive.

Both the Office of the Chief Information and the Privacy Commissioner will be conducting an investigation.

s.13

Formatted: No Spacing, Line spacing: single, No bullets or numbering

Comment [TS1]: TBC

- **The Office of the Chief Information Officer is conducting its own investigation of core government compliance with policies around personal information management.**

Formatted: Font: (Default) Calibri, 14 pt, Bold

This will give us an understanding of how this happened and the ability to make mandatory recommendations to prevent such an incident from happening again.

Formatted: Font: (Default) Calibri, 14 pt, Bold

The Privacy Commissioner has also initiated a formal investigation.

Formatted: Font: (Default) Calibri, 14 pt, Bold

Secondary Messages – Data

Background

- **The Ministry of Education is unable to locate an unencrypted external hard drive with a variety of reports, databases, and information.**
- **The hard drive contains 3.4 million personal records that include in various formats, names, grades and in some cases addresses.**
- **The hard drive does not contain social insurance numbers, personal health numbers, driver's licence or banking information.**
- **The Ministry of Education continues to carry out an extensive search for the hard drive.**

FOR INTERNAL USE ONLY Questions and Answers
Missing Hard Drive
Sept. 22, 2015

1. What are you announcing today?

- The Office of the Chief Information Officer will review the management of personal information by government ministries after the Ministry of Education was unable to locate an unencrypted external hard drive with a variety of reports, databases, and information.
- Service BC operators will also be able to help British Columbians and others if their information is likely on the drive, and what sort of information it would be.
- Some of the files on the hard drive contain some personal information, like names, postal codes, grades, and in some cases addresses.
- What it does not contain are 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 by someone or misused in any way, government is alerting the public out of an abundance of caution because the hard drive has not been located.
- We continue to look for the missing hard drive and any record of its whereabouts.

2. What is missing?

- s.15
-
- This hard drive is one of two external hard drives that the ministry used to store ministry records.
- The original was in the possession of the ministry and used to determine the kind of information on the misplaced duplicate drive. The original was handed over to the Office of the Chief Information Officer on Sept. 20.
- It's important to note that the ministry has all student records available and securely stored. The misplaced drive was a backup created for emergency use only.

3. How did you discover the disk was missing?

- The issue of the backup drives and their content was discovered during a records review undertaken by the Ministry of Education to ensure it was in compliance with data storage standards.

- In mid-August, based on anecdotal information staff went to the warehouse to collect the offsite duplicate drive so it could be destroyed. When the drive couldn't be located, a search of the warehouse and electronic records was launched.

- On August 28, 2015, a record in government's records management system was located, the first formal confirmation of the existence of the duplicate drive.

4. When was the hard drive last seen?

- In May 2011 when it was created and a record placed in the government record management system.

5. What steps have been taken to locate the hard drive?

- There have been five full searches of the warehouse, each one more thorough and detailed, including opening shrink-wrapped boxes throughout the large facility.

- The Ministry of Education has done a full search of its offices, including storage, public, and personal areas.

- The ministry's storage and destruction records have been scrutinized for any record of the hard drive.

6. Have any other items been found to be missing?

- No.

7. What kind of information is on the drive?

- The drive was created and stored offsite in case of a disaster so education data would continue to be available.
- There are 8,766 folders and 138,830 files on the hard drive.
- In total, there are 3.4 million personal records of varying types in different documents and ranging from 1986-2009.
- These records include names, postal codes, grades, and personal education numbers.
- There are also a smaller number of records in files that include more sensitive personal information, such as:
    - 825 survey results from 2003 of teachers aged 53 or older on their retirement plans;
    - 1,052 personal education numbers, birth years, and grad dates for cancer survivors from a study on their education outcomes;
    - 9,273 personal education numbers connected to children in the care of the Ministry of Children and Family Development before 2006/07, including information such as health and behaviour issues and supervision status.
- Full details of the data on the disc are available online.

8. Why does government have this kind of information?

- 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.

9. Has this data been accessed?

- There is no evidence that the data on the missing hard drive has been accessed or used.
- We are making this situation public out of an abundance of caution as we have been unable to locate the hard drive.
- There is a chance, however slight, that the duplicate hard drive is inside a box somewhere in government storage, or that the hard drive has been destroyed.

10. Were correct procedures followed in creating and storing this hard drive?

- No. Neither the creation nor storage of the hard drive meets government information security policies of either the time it was created or now.
- This hard drive was created in 2011. Much has changed since then and most of our records are now stored electronically on secure servers in Kamloops and Calgary.
- Government policy requires that only in limited circumstances should information be stored on a portable IT device, and where this is done the device must be encrypted.
- Government's Information Security Policy requires encryption be used and stored in a secure location with security that matches the sensitivity of the information stored on it.

11. Will any staff be disciplined?

- We are still looking into what happened – it would be inappropriate to speculate.

12. What can you tell me about where it was stored?

- The warehouse where we think the hard drive was last stored is 11,483 square feet in size and is secured with a key lock and an alarm system.
- The site is primarily used for processing and storing ministry administered exams and out of date textbooks and was not intended to be an offsite storage facility.
- The Ministry of Education continues to carry out an extensive search of its facilities, and is following up in other locations where files are stored.

13. How are student records and other types of personal information archived and protected?

- Government takes the management of information and the protection of privacy very seriously.
- We have safeguards in place to protect the security of government data and personal information.
- B.C. has some of Canada's most stringent legislation to protect personal information.
- For example, government stores archive computer files on secure servers in a secure data facility (Kamloops Data Centre) and paper files are archived in secure storage facilities.

14. What are you doing about it and will there be a review?

- The incident has been reported to the Office of the Chief Information Officer, which is conducting an investigation into the incident. This investigation will not be made public.
- In addition, a review of the management of personal information by government ministries compliance with policies around personal information management will be undertaken by the same office. That review will be made public.
- The Ministry of Education will be reviewed first.
- The Information and Privacy Commissioner was notified on Sept 18 and is conducting its own investigation.
- The Ministry of Education continues to carry out an extensive search of its facilities, and is following up in other government locations where files are stored.

15. How could this happen?

- A mistake was made – both in creating the two hard drives as backups, and in how they were stored.
- Government takes the management of information and the protection of privacy very seriously.
- We have safeguards in place to protect the security of government data and personal information.
- There are instances where an employee doesn't know the policy because they are new or the employee doesn't understand how it applies to them and in rare occasions they may choose to ignore it.
- Government is working hard to reduce the number of breaches that occur through mandatory training and education, and breaches are down slightly as a result.
- At present, 72% of all government employees have completed the mandatory Information Sharing and Privacy Awareness training.
- To be clear - this hard drive should have been encrypted at a minimum and it should not have been stored at this warehouse.
- Again, we have no evidence to suggest that the hard drive has been accessed or misused in any way.

OIPC Reporting

16. Why did it take you three weeks to notify the Privacy Commissioner?

- The Ministry of Education signalled that the hard drive was missing as soon as it knew the type of information on the hard drive combined with the likelihood it was missing reached a critical point.

- The search of the warehouse continued – and escalated – but we were not aware of the contents of the hard drive as the files had not been analyzed.

- The Ministry of Education first notified the Office of the Chief Information Officer a backup hard drive was missing on Sept. 1.

- When the Ministry of the Education became aware that the missing hard drive contained a large volume of student personal information on Sept. 14 the Office of the Chief Information Officer was immediately notified.

- Efforts to locate the missing drive intensified at that point. We launched a deeper and broader physical search, as well as a detailed analysis of the more than 130,000 files on the hard drive.

- Formal notification to the Office of the Information and Privacy Commissioner happened on Friday, September 18 through the Office of the Government Chief Information Officer.

- A team of between 30 and 90 people authorized and trained reviewed each file from the original hard drive Sept 18-20 to determine the data on the missing hard drive.

17. How can you say you take people's privacy seriously when you waited three weeks to notify the public?

- We notified the Privacy Commissioner as soon as the scope of the information on the hard drive became apparent, and the extensive searches for the backup drive were fruitless.
- The ministry wanted to ensure that it undertook a methodical and thorough search for the hard drive before unnecessarily raising an alarm.
- Once a very thorough search had been conducted, we determined that it was necessary to inform the public and the Office of the Information and Privacy Commissioner and that's what we've done.
- We have no evidence that the hard drive has been accessed or misused. We have lost track of the hard drive but we also don't know that it's not in government custody.
- We continue to search for the hard drive, and out of an abundance of caution we are treating it like a potential privacy breach and notifying the public.

18. At what point did you know the actual volume of records that were missing?

- The Ministry of the Education became aware that the missing hard drive contained a large volume of student personal information on Sept. 14.
- A team of more than 28 people reviewed each file from the original hard drive Sept 18-20 to determine the data on the missing hard drive.
- When it appeared that the drive was unlikely to be located, it was determined that the incident needed to be reported to the Office of the Information and Privacy Commissioner and the public.

19. So you knew millions of people's records were at risk and you took three more days to notify the Privacy Commissioner?

- We had to complete our due diligence to confirm the kind of data on the missing hard drive, and to complete an extensive and thorough search.
- We reported it to the Privacy Commissioner on Sept. 18 - as soon as we knew the type of information on the hard drive combined with the likelihood it was missing reached a critical point.

20. What is the reporting requirement to the OIPC?

**** note there is no legislated requirement to report incidents to the OIPC***

- Government reports all privacy breaches to the OIPC.
- Serious privacy breaches are reported to the OIPC as soon as possible. Serious breaches typically involve a large number of impacted people and the potential for serious harm.
- Government also reports to the OIPC on a monthly basis, with all actual or suspected government privacy breaches.
- A recent report by the Information and Privacy Commissioner found that government has a strong privacy breach management process.
- Government is working hard to reduce the number of breaches that occur through training and education and breaches are down slightly as a result.
- At present, 72% of all government employees have completed the mandatory Information Sharing and Privacy Awareness training.
- The new Privacy Management and Accountability Policy strengthens practices already in place and is scheduled to be released in the next few weeks and clearly sets out how government as a whole manages privacy.

21. The reporting requirement seems be left to the whim of government, do you have any plans to change that?

- Government reports all privacy breaches to the Office of the Information and Privacy Commissioner.
- Concerns such as this can be put to the Special Committee reviewing the Freedom of Information and Protection of Privacy Act. We welcome any such discussion by the Special Committee.

Privacy Commissioner Report Feb. 2015

22. What is the status of the Commissioner's recommendations, how many have been implemented?

- We are taking action on these recommendations.
- The OCIO has taken action to address a number of the OIPC's recommendations and work is underway to address the remaining initiatives.
- The OCIO and OIPC have agreed that government will continue to report serious breaches within a few days of discovering the incident.
- In addition, the OCIO is also providing a report to the OIPC, on a monthly basis, which provides information about all actual or suspected privacy breaches reported to the OCIO.

General Records Management Policy

23. Where should the hard drive have been stored?

- Should a ministry elect to use a portable storage device it is responsible for determining the location where the device will be stored.
- These decisions must be made in accordance with government policy which requires that the device be encrypted and stored in a secure location commensurate with the sensitivity of the information stored on the device.

24. This was an unencrypted hard drive, what is government's policy around proper hard drive storage?

- This hard drive was created in 2011. Much has changed since then and most of our records are now stored electronically on servers in Kamloops and Calgary.
- Government policy requires that only in limited circumstances should information be stored on a portable IT device, and where this is done the device must be encrypted.
- Government's Information Security Policy requires encryption be used and stored in a secure location with security that matches the sensitivity of the information stored on it.

25. What are you doing to ensure other records aren't missing?

- There is no doubt that the storage procedure followed in this particular case was incorrect and did not follow proper policy at the time.
- It was inappropriate to store an unencrypted hard drive which contained a large volume of personal information at an offsite location with little mechanism to track the device.
- We are confident that this is an isolated incident and is not part of a larger problem.
- Our policy has been updated since this hard drive was stored and the Province continues to have effective practices and policies in place.

26. What checks and balances are in place to ensure privacy breaches don't occur?

- The Document Disposal Act and its replacement, the Information management Act, together with the Freedom of Information and Protection of Privacy Act will provide the foundation for how public bodies must collect, use, store, disclose and destroy personal information.
- Government has a robust set of information security policies and procedures in place to provide further guidance to staff about the handling of personal information.
- As more employees have become aware of responsibilities with respect to privacy breaches, there was an increase in the number of breaches reported between 2010 and 2014.
- This year, for the first time since the Information Incident Management Process was established in 2010, the number of privacy breaches has decreased.
- Government is working hard to reduce the number of breaches that occur through training and education and breaches are down slightly as a result, compared to last year.
- Staff is required to attend mandatory privacy and security training so that expectations are clearly communicated and understood.
- In addition, as part of each privacy breach investigation, the OCIO seeks to identify measures that the program area can implement to prevent similar incidents from happening in future.
- The OCIO conducts monthly privacy audits on ministries on implementation of prevention measures issued as part of privacy investigations.
- Approximately 73% of all breaches reported to the OCIO are administrative errors, which are minor, human error based incidents that typically only impact one individual.

27. How many hard-drives has each ministry lost?

- The Office of the Chief Information Officer tracks privacy incidents which involve lost/missing items.
- All information incidents must be reported.
- There is a formal reporting process that must be followed in responding to incidents that threaten privacy or security.
- Over the last five years, there have been three hard drives that were lost and contained personal information. One was eventually recovered.

28. How does this breach compare to previous ones in terms of the number of records impacted?

- It's important to keep in mind that there is no evidence at this time to suggest that the information has been accessed by someone or misused in any way.
- That said, this potential privacy breach impacts approximately 3.4 million personal records and would be the largest in recent years.

If pressed for previous, comparable breaches:

- Most recently, in 2014, a Wildfire Management Branch database which contained information about approximately 15,000 wildfire firefighters was accessed by an unauthorized individual.
- So by comparison this is a much larger potential breach but I think you'll find that on the whole, government security breaches are small compared to some of the private sector breaches we've seen.
- For instance, the US Postal Service was hacked exposing more significant personal information of 3.7 million people.
- Similarly, 65 million Home Depot credit cards were exposed in a data breach last year.

29. How many other similar breaches have there been over the last 10 years?

- Over the last five years, there have been three hard drives that were lost and contained personal information. One was eventually recovered.
- Since 2010, a total of 4,420 government privacy breaches have been reported to the Office of the Chief Information Officer.
- This trend was increasing through 2014, but has since begun to decline as BC Public Service employees have become aware, through training and awareness activities, of the need to report all actual or suspected privacy breaches and other information incidents.

30. What safeguards are in place in Government to protect data?

- Government has robust information security controls.
- Government workstations are centrally configured and policies ensure the security of government's information.
- Encryption technologies ensure only authorised users are able to logon to workstations and only they can access their own data.
- User data is stored on centrally managed servers with minimal information residing on government workstations.
- Anti-virus and anti-malware is centrally managed and updated regularly.
- All government data is removed from workstations prior to disposal.
- Mobile devices such as smartphones and tablet devices have password protection and data encryption and can be remotely 'wiped' should they be lost or stolen.

31. Clearly, proper procedures weren't followed. What training is offered to employees?

- Government's goal and ongoing efforts are focused on reducing the number of breaches that occur.
- If an incident does occur, we want to ensure government responds quickly – and there is clarity among staff with respect to the steps they should take to report an incident.
- Work is ongoing, through the development of new policies and training, to ensure government and employees know what to do when an incident occurs.
- All staff must complete mandatory privacy awareness training.

- The OCIO is developing new privacy training courses for government contractors and service providers and is developing a new privacy professional certification training program which will incorporate records management, security and privacy requirements.

- The new Privacy Management and Accountability Policy will strengthen practices already in place and is scheduled to be released in the next few weeks. It clearly sets out how government as a whole manages privacy in one policy.

- Government is working hard to reduce the number of breaches that occur through training and education and breaches are down slightly as a result.

32. What checks and balances are in place to know that employees are following procedures?

- Government has a strong framework in place for the centralized reporting of incidents to the OCIO.

- If an incident does occur, we want to ensure government responds quickly – and there is clarity among staff with respect to roles, responsibilities and reporting structure.

- Employees must take a mandatory privacy and awareness course.

- Work is ongoing, through the development of new policies and training, to ensure government and agency staff know what to do when an incident occurs.

- As a result, breaches are down slightly and we are also seeing an increase in the number of reported breaches.

- The OCIO is also developing a privacy audit program, and has begun auditing the implementation of OCIO recommendations issued during the course of privacy investigations, and will have ministries complete yearly self-audits as a mechanism to improve privacy compliance.

Impact to Public

33. What is the risk to the public or the worst case scenario?

- We continue to assess the risk to British Columbians and it's important we don't jump to conclusions.
- I want to emphasize that we presently have no reason to believe that the missing hard drive is in the wrong hands or has been misused.
- With a potential data breach of this nature, there is a risk of identity theft or fraud, however, we think that risk is low because data is spread across different files.
- The data on this hard drive does not include social insurance numbers, banking information, driver's licence or personal health numbers.
- Many of the addresses will also be outdated by now.
- People are always encouraged to use good personal information management practices such as checking their account statements and calling Canada's national credit agencies if they suspect their personal information has been put at risk.

34. What are you doing to notify individuals?

- This is the first step of the notification process – by telling media.
- We will also use social media to spread the word and we'll work with our education partners to connect share our notification with as many parents and students as possible.
- The OCIO is continuing to investigate and is consulting with the Office of the Information and Privacy Commissioner. As we learn more about the data on the hard drive we will adapt our notification process as necessary.

35. How do I find out if my personal information is stored on this drive?

- Individuals can contact Service BC to find out if their information is likely on the drive, and what sort of information it would be.
- Call centre staff will be able to tell them what type of data (name, postal code, etc.) could be on the missing hard drive, as well as any privacy steps they could take.
- People can call: **1-800-663-7867** from 7:30 a.m. - 5 p.m. Monday to Friday.
    - Victoria: 250-387-6121
    - Vancouver: 604-660-2421

36. Do you know if anyone's information has been compromised?

- We have no evidence at this time to suggest that the information has been accessed by someone or misused in any way.

37. Is there anything people should do themselves?

- We continue to assess the risk to British Columbians.
- I want to emphasize that we presently have no reason to believe that the missing hard drive is in the wrong hands or has been misused.
- With a potential data breach of this nature, there is a risk of identity theft or fraud, however, we think that risk is low.
- We encourage people to use good personal information management practices such as checking their account statements and calling Canada's national credit agencies if they suspect their personal information has been put at risk.
- If they have proof their identity has been stolen, they should call the police.

38. How will the public know if their information has been compromised?

- We presently have no reason to believe that the missing hard drive is in the wrong hands or has been misused.
- We will notify people if we have any reason to believe there is further risk.
- People are always encouraged to use good personal information management practices such as checking their account statements and calling Canada's national credit agencies if they suspect their personal information has been put at risk.

39. Have you notified the police and if not, why?

- We presently have no reason to believe that the missing hard drive is in the wrong hands or has been misused. We therefore have no basis upon which to notify the police.
- We will notify people if we have any reason to believe there is further risk.
- Should new information come forward, we would notify police if deemed appropriate.

O'Connor-Dixon, Lara EDUC:EX

From: Byng, Dave A EDUC:EX
Sent: Tuesday, September 22, 2015 11:18 AM
To: EDUC DL Ministry All
Subject: Update on Potential Data Breach

Follow Up Flag: Follow up
Flag Status: Flagged

To All Staff,

As you may be aware, we have been conducting a comprehensive search for an unencrypted external hard drive containing student level data. I wish to thank everyone who participated in the extensive physical search of the ministry's Victoria facilities, as well as acknowledge the countless staff who spent time away from their family and friends this past weekend to help complete a detailed analysis of the content on the drive.

While there is no evidence to suggest that the information has been improperly accessed or misused in any way, out of an abundance of caution, government is informing the public today that the hard drive has not yet been located.

Please refer to this news release and backgrounder for more information.
http://www2.news.gov.bc.ca/news_releases_2013-2017/2015MTICS0026-001575.htm

In these times, we are all reminded how important it is to protect government's information assets. As public servants, each of us is responsible for understanding our roles and responsibilities with respect to data protection and government's core polices. I recognize that the majority of staff have already completed the course titled "**Privacy and Information Sharing: Awareness Training**"; for those of you who may not have completed this course already, please complete this mandatory training (steps for registering are appended to this note).

If you are contacted by our partners in the sector, the public or media with questions about this incident, please be reminded of the following protocols:

- All questions from the public or sector partners are to be directed to the Service BC's Contact Centre at:
  - Victoria: 250-387-6121
  - Vancouver: 604-660-2421
  - Elsewhere in B.C.: 1-800-663-7867
- If for any reason media contact staff, please direct them to the Government Communications and Public Engagement office at 250-356-5963.

On behalf of our executive team, I want to once again acknowledge and thank the many staff who supported the analysis over the weekend.

Please do not hesitate to direct any questions you may have to your immediate supervisor, or any member of the executive team.

Sincerely,

Dave Byng
Deputy Minister

Nugent, Tim EDUC:EX

From: Vinning, Gurpreet S EDUC:EX
Sent: Tuesday, September 22, 2015 11:20 AM
To: Nugent, Tim EDUC:EX; O'Connor-Dixon, Lara EDUC:EX
Subject: Fwd: Issue Alert: Missing Hard Drive

See below.

Sent from my Samsung Galaxy smartphone.

-------- Original message --------
From: "Grimsrud, Tracy" <Tracy.Grimsrud@leg.bc.ca>
Date: 09-22-2015 11:17 AM (GMT-08:00)
To:
Subject: Issue Alert: Missing Hard Drive

Issue Alert: Missing Hard Drive

The Ministry of Education discovered that an unencrypted external hard drive with personal student information was missing from a government storage unit in Victoria.

The hard drive contains K-12 student names, Foundational Skill Assessments (FSA) ratings, birthdates, home addresses, grades and personal education numbers.

What it does not contain are 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 by someone or misused in any way, government is responding to the incident as a potential privacy breach because the hard drive has not been located.

We continue to look for the missing hard drive, and out of an abundance of caution we are informing the public about this potential privacy breach.

Lead: Ministry of Technology, Innovation and Citizens' Services

Key Messages:

- Government takes the management of information and the protection of privacy very seriously.
- At this point, we are not aware of any access to, or use of the information on the disk. We cannot locate the unencrypted backup disk – it may be misplaced or it may have been destroyed.
- British Columbians can find out if their information is on the hard drive by calling Service BC.
- The Office of the Chief Information Officer is conducting its own review of core government compliance with policies around personal information management.
- This will give us an understanding of how this happened and the ability to make mandatory recommendations to prevent such an incident from happening again.
- The Privacy Commissioner has initiated a formal investigation.

Background:
The Service BC contact centre is able to help British Columbians and others find out if their information is likely on the drive, and what sort of information it would be.

When they contact Service BC, people should be able to note when they attended K-12 or post-secondary school in British Columbia. The contact centre is open Monday to Friday from 7:30am to 5pm and can be reached by calling:

- Victoria: 250-387-6121
- Vancouver: 604-660-2421
- Elsewhere in B.C.: 1-800-663-7867

In total, on a number of files on the drive, there are about 3.4 million education records tied to an individual between 1986 and 2009, including their names, postal codes, grades, and personal education numbers.

There are also a smaller number of records in files that include more sensitive personal information, such as:

- 825 survey results from 2003 of teachers aged 53 or older on their retirement plans;
- 1,052 personal education numbers, birth years, and grad dates for cancer survivors from a study on their education outcomes;
- 9,273 personal education numbers connected to children in the care of the Ministry of Children and Family Development before 2006/07, including information such as health and behaviour issues and supervision status.

This sensitive information could be connected to names by comparing the personal education numbers to names through the larger data file.

Link to news release: http://ow.ly/Sxcnl

Tracy Grimsrud
Senior Communications Officer & Audio/Visual Producer
BC Government Caucus
Phone: (250) 387-0868
Fax: (250) 387-7957
Cell: (250) 213-1554

Connect with Caucus:
www.governmentcaucus.bc.ca
www.twitter.com/BCLiberalCaucus
www.youtube.com/BCGovCaucus

Delisle, Corrie EDUC:EX

From: Keenan, Jason GCPE:EX
Sent: Friday, September 25, 2015 11:52 AM
To: Delisle, Corrie EDUC:EX; Vinning, Gurpreet S EDUC:EX
Cc: Lowther, Brett GCPE:EX
Subject: FW: MTICS Media Request - CJDC - Missing Hard Drive

MAV is doing this interview this afternoon

Deadline @ **3pm**

Media: CJDC TV - Dawson Creek

Reporter: Ashley Wiebe, s.22

Topic: Missing Hard Drive

Background: Reporter would like an interview with Minister Bernier on camera but will take a phone interview.

Suggested Response:

Could you explain what was on the hard drive that is missing? What do parents and teachers need to know?

- **The Office of the Chief Information Officer will review the management of personal information by government ministries after the Ministry of Education was unable to locate an unencrypted external hard drive with a variety of reports, databases, and information.**
- **Some of the files on the hard drive contain some personal information, like names, postal codes, grades, and in some cases addresses.** Full details of the data on the disc are available online.
- **What it does not contain are 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 by someone or misused in any way, government is alerting the public out of an abundance of caution because the hard drive has not been located.**
- **We continue to look for the missing hard drive and any record of its whereabouts.**
- **People can contact Service BC to find out if their information is likely on the drive, and what sort of information it would be.**
- **Call centre staff will be able to tell them what type of data (name, postal code, etc.) could be on the missing hard drive, as well as any privacy steps they could take.**
- **People can call: 1-800-663-7867 from 7:30 a.m. - 5 p.m. Monday to Friday.**

Tell us about the timeframe that the hard drive went missing and when it was discovered.

- **The issue of the backup drives and their content was discovered during a records review undertaken by the Ministry of Education to ensure it was in compliance with data storage standards.**

- **In mid-August, based on anecdotal information staff went to the warehouse to collect the offsite duplicate drive so it could be destroyed. When the drive couldn't be located, a search of the warehouse and electronic records was launched.**

- **On August 28, 2015, a record in government's records management system was located, the first formal confirmation of the existence of the duplicate drive.**

- **The Ministry of the Education became aware that the missing hard drive contained a large volume of student personal information on Sept. 14.**

- **A team of more than 28 people reviewed each file from the original hard drive Sept 18-20 to determine the data on the missing hard drive.**

- **When it appeared that the drive was unlikely to be located, it was determined that the incident needed to be reported to the Office of the Information and Privacy Commissioner and the public.**

- **The Ministry of Education continues to look for the missing hard drive and any record of its whereabouts.**

Tasha Schollen | Communications Director
Ministry of Technology, Innovation and Citizens' Services
Government Communications and Public Engagement
Phone: 250-387-3134 | Cell: 250-889-1121

Delisle, Corrie EDUC:EX

From: Facey, Nick MTIC:EX
Sent: Wednesday, September 23, 2015 3:42 PM
To: Southern, Evan PREM:EX; Mills, Shane LASS:EX
Cc: Ingram, Geoff MTIC:EX; Delisle, Corrie EDUC:EX
Subject: Fwd: Media Request - News 1130/Times Colonist - Missing hard Drive Credit Protection

Okay to send background to both reporters?

Deadline @ **asap**

Media: News 1130

Reporter: Jill Drews, s.22

Topic: Missing Hard Drive – Credit Protection

Background: Reporter would like to know if the province is considering providing credit protection to the people who's records are on the missing hard drive. She says that the federal government did this when there was a student loan breach.

Questions: **Is government considering getting people whose data is on the missing hard drive credit protection?**

Deadline @ asap

Media: Times Colonist

Reporter: Lindsay Kines s.22

Topic: Missing Hard Drive – Credit Protection

Background: Reporter would like to know if the province is considering providing credit protection to the people whose records are on the missing hard drive. He says that in 2012, when someone stole an unencrypted storage device from UVIC, the university reached a deal with TransUnion and Equifax to provide credit monitoring services free of charge for the nearly 12,000 employees affected by the exposure of their personal and banking information.

Questions: I'm wondering whether such an arrangement was considered in this latest breach in MOE and why it wasn't offered to the 3.4 million people affected?

Suggested Response:

- **We continue to assess the risk to British Columbians.**
- **With a potential data breach of this nature, there is a risk of identity theft or fraud.**
- **We want to emphasize that we presently have no reason to believe that the missing hard drive is in the wrong hands or has been misused.**
- **We continue to assess potential harms and will consider credit monitoring services if warranted.**
- **We encourage people to use good personal information management practices such as checking their account statements and calling Canada's national credit agencies if they suspect their personal information has been put at risk.**
- **If they have proof their identity has been stolen, they should call the police.**

Tasha Schollen | Communications Director

Ministry of Technology, Innovation and Citizens' Services

Government Communications and Public Engagement

Phone: 250-387-3134 | Cell: 250-889-1121