



4 June 2025

s 9(2)(a)

Dear s 9(2)(a)

Thank you for your request made under the Official Information Act 1982 (OIA), received on 11 April 2025. You requested the following:

Since January 1 2020, copies of all reports, briefings, documents and emails relating to any incidents when material or items were mistakenly left unaccompanied in public. The information sought in this request is to be used as part of a report by Stuff.

Inland Revenue takes its confidentiality requirements seriously, and has processes in place to safeguard the information it holds. This includes processes for these incidents to be reported and acted on quickly, and the ability to remote wipe Inland Revenue devices. When incidents do occur, we attempt to recover the information and where appropriate consider how similar occurrences could be prevented from taking place in the future.

Information being released

The details of 13 incidents involving material or items left unaccompanied in public are provided in the table below.

Table 1 – Material or items left unaccompanied in public from 1 January 2020 – 11 April 2025

| Item | Date | Incident description | Resolution description |
|------|------------|---|---|
| 1. | 19/04/2022 | Encrypted USB lost between IR workplace and employee's private vehicle. | USB not located, police notified. |
| 2. | 22/09/2022 | IR laptop and training notes left in a hospitality venue outside of work hours. | Laptop remotely wiped, collected from venue the next day. |
| 3. | 29/07/2022 | IR mobile phone left on train. | Mobile phone remotely wiped. |
| 4. | 29/01/2023 | IR laptop left on bus. | Laptop remotely wiped. |

| Item | Date | Incident description | Resolution description |
|------|------------|---|---|
| 5. | 12/05/2023 | IR mobile phone lost. | Mobile phone remotely wiped. |
| 6. | 16/05/2023 | IR laptop and access card left on bus. | Laptop and access card remotely wiped/cancelled, collected from bus company 3 days later. |
| 7. | 04/12/2023 | IR mobile phone lost. | Mobile phone remotely wiped. |
| 8. | 13/12/2023 | IR laptop left at another government agency office. | Laptop remotely wiped. |
| 9. | 17/05/2024 | Folder containing customer information left at a hospitality venue outside of work hours. | Folder collected from venue. |
| 10. | 14/06/2024 | IR mobile phone lost. | Mobile phone remotely wiped. |
| 11. | 22/07/2024 | IR mobile phone lost. | Mobile phone remotely wiped. |
| 12. | 01/08/2024 | IR mobile phone lost. | Mobile phone remotely wiped. |
| 13. | 17/02/2025 | IR Mobile phone lost. | Mobile phone remotely wiped. |

Please find enclosed 268 emails and 30 documents within scope of your request as **Appendix A, B, C, D, E and F**. Some information has been assessed as outside the scope of your request and has therefore been excluded or redacted as *Out of scope*. Additionally, certain duplicated content has been withheld and marked as *Out of scope – duplicate*.

I am releasing the relevant portions of the documents that fall within the scope of your request with some information withheld under the following sections of the OIA, as applicable:

- 9(2)(a) – to protect the privacy of natural persons, including deceased people.
- 9(2)(g)(i) – to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or officers and employees of any public service agency in the course of their duty,
- 9(2)(h) – to maintain legal professional privilege.
- 18(c)(i) – where making the requested information available would be contrary to the provisions of a specified enactment, namely Inland Revenue's confidentiality obligations

in section 18(1) of the Tax Administration Act 1994 (TAA). Further, section 18(3) (in conjunction with section 143C(1)(a) of the TAA) prevents the Commissioner of Inland Revenue from disclosing any item of revenue information if the release of the information would adversely affect the integrity of the tax system or prejudice the maintenance of the law.

As required by section 9(1) of the OIA, I have considered whether the grounds for withholding the information requested is outweighed by the public interest. In this instance, I do not consider that to be the case.

Right of review

If you disagree with my decision on your OIA request, you have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the OIA. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Publishing of OIA response

We intend to publish our response to your request on Inland Revenue's website (ird.govt.nz) as this information may be of interest to other members of the public. This letter, with your personal details removed, may be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the OIA's purpose of enabling more effective participation in the making and administration of laws and policies and promoting the accountability of officials.

Thank you again for your request.

Yours sincerely

s 9(2)(a)



David Carrigan

Acting Chief Security Officer

Appendix A

Initial report received from Murray Deadman

Friday, September 23, 2022 1:14 PM

1.Name: Murray Deadman

2.How can we contact you: s 9(2)(a) or via teams.

3.What is happening that concerns you: One of my team left their laptop, in a laptop bag, and some training notes at a premises last night. They rang this morning but the bag has not been handed in. The training notes do not identify any particular customer(s) they cover what should be looked at when looking into a customers financial position.

4.Where is it happening:Trax Tavern Wellington approx 9:45 pm on 22/09/2022.

5.Who is involved: s 9(2)(a) from my team.

6.Are they staff members: Yes

7.Is there any evidence to support your concern: No

8.Details of people who can provide further information:

9.Do they know you have reported this: Yes

10.Have you previously reported these concerns: No

11.Is there anything else we need to know: No

From: Integrity WIPs s 18(c)(i)

Sent: Friday, 23 September 2022 2:21 pm

To: Murray Deadman s 9(2)(a)

Cc: Integrity WIPs s 18(c)(i)

Subject: RE: New Report of Wrongdoing

Kia ora Murray,

Thanks for sending this through, can you please confirm that the following Support Portal form has been submitted: [Report Lost or Stolen Devices](#)

I have also been in touch with Corporate Security who have confirmed that a SID needs to be raised in START.

The instructions can be found in Te Mātāwai page: [Reporting security incidents](#)

You will need to start from key point 2 as this is a non-customer specific incident.

Thanks,

Fune Parsons ([he/him](#))

From: Iosia Misa s 9(2)(a)

Sent: Friday, 23 September 2022 3:18 pm

To: Ross Walker s 9(2)(a); Fune Parsons s 9(2)(a)

Subject: RITM0233664 Device - L-035644682353 Confirmed Stolen

[UNCLASSIFIED]

Good Afternoon Ross,

FYI for your Team.

Report a lost or stolen IR Device

Details

If you are raising this request on behalf of another user, please select them below: s 9(2)(a)

Select device: Laptop

Select approximate time and date the device was lost or stolen: 2022-09-22 21:45:00

Do you have START access?: true

Where was the device last seen?: Trax Tavern Wellington

What steps have you taken to recover the device?: The staff member has rung the Tavern and they do not have it.

Has the loss or theft been reported to the Police?: No

Do you need a replacement device?: Yes

Please provide delivery instructions and any additional details: Level 1 110 Featherston St
Wellington. 021 179-1151

Action Taken

1. Confirm the device make model, Surface Pro – Host Name : L-035644682353 and advise the User for the Police report. (Work in progress – Fune has been advised by Murray Deadman – Report will be up loaded into the Ticket.
 2. IR Tech Team has Wiped the device.
 3. If appropriate locate the SIM number for cancellation.
 4. Update close notes with your findings in detail so other teams can complete their tasks.
-

From: Jay Harris s 9(2)(a)

Sent: Tuesday, 27 September 2022 8:02 pm

To: Vanessa Johnson s 9(2)(a) ; Joanne Petrie
s 9(2)(a) ; Ta'au Savaiinaea s 9(2)(a) ; Rowan McArthur
s 9(2)(a) ; Gay Cavill s 9(2)(a) ; Ross Walker
s 9(2)(a)

Subject: FW: Lost Laptop

FYI, below is the response I received from SecOps on this issue. This information is based on what is recorded in SNoW. I note that the incident ticket Jo sent through did not look like a SNoW identifier....do we have a disconnect between multiple incident recording systems? Has anyone touched base with the individual to verify that it was actually found and is back in there possession?

Jay

From: Jay Harris s 9(2)(a)

Sent: Tuesday, 27 September 2022 7:52 pm

To: Jay Harris s 9(2)(a)

Subject: Lost Laptop

Hi Jay,

Went through he logs on the ticket. The laptop has been found same day. Sec ops was not notified of any action or assigned any action item.

Sent from my iPhone

From: Ta'au Savaiinaea s 9(2)(a)

Sent: Wednesday, 28 September 2022 8:31 AM

To: Jay Harris s 9(2)(a); Vanessa Johnson s 9(2)(a);
Joanne Petrie s 9(2)(a); Rowan McArthur s 9(2)(a);
Gay Cavill s 9(2)(a); Ross Walker s 9(2)(a)

Subject: RE: Lost Laptop

Hi All

I just spoke with Murray Deadman (Team Lead) for s 9(2)(a) (staff member who lost the laptop). Murray advised that the laptop has not been found and will contact Integrity when/if the laptop has been found.

Jason Deng (Service Integration & Delivery) confirmed with Integrity that the laptop was wiped at 2:54:40pm 23/09/2022.

Kind Regards

From: Vanessa Johnson s 9(2)(a)

Sent: Wednesday, 28 September 2022 8:35 am

To: Ta'au Savaiinaea s 9(2)(a); Jay Harris s 9(2)(a); Joanne Petrie
s 9(2)(a); Rowan McArthur s 9(2)(a); Gay Cavill
s 9(2)(a); Ross Walker s 9(2)(a)

Subject: RE: Lost Laptop

Ok

This is very odd.

Based on when the lap top was wiped are you comfortable with letting the integrity process continue and monitor the media just in case. Ta'au – can you see if Jason Deng can confirm that the lap top had not been accessed either.

I would like to pass this example on to the team working on improving our incident mgt process



Regards

Vanessa

From: Ross Walker s 9(2)(a)

Sent: Wednesday, 28 September 2022 9:07 am

To: Vanessa Johnson s 9(2)(a); Ta'au Savaiinaea s 9(2)(a); Jay Harris s 9(2)(a); Joanne Petrie s 9(2)(a); Rowan McArthur s 9(2)(a); Gay Cavill s 9(2)(a)

Subject: RE: Lost Laptop

Good morning,

Apologies for missing yesterday's meeting.

As this is an Inland Revenue asset we should explore the possibility of recovering it or holding someone to account for the theft (if it is theft).

I have spoken to Ta'au and have some contacts at the facility the machine was last seen in so will do some work to establish if there are any avenues of enquiry.

Regards

Ross

Ross Walker

Domain Principal

Corporate Security

Organisational Resilience

From: Ross Walker s 9(2)(a)

Sent: Friday, 30 September 2022 9:39 am

To: Jay Harris s 9(2)(a) ; Vanessa Johnson s 9(2)(a) ;
Joanne Petrie s 9(2)(a) ; Ta'au Savaiinaea s 9(2)(a) ; Rowan
McArthur s 9(2)(a) ; Gay Cavill s 9(2)(a)

Cc: Murray Deadman s 9(2)(a) ; Nick Tomlin s 9(2)(a)

Subject: Lost Laptop

Good morning,

I visited Trax this morning to establish whether they might have CCTV footage of the incident.

They had the bag and I have recovered it.

It has been locked away in the managers office and the information has not been compromised.

Regards

Ross

Ross Walker

Domain Principal

Corporate Security

Organisational Resilience

Final report received from Mark Dawson-Mau'u

Thursday, February 23, 2023 5:13 PM

1.Case Number: 20222087

2.Email address for confirmation: s 9(2)(a)

3.Your Name: Mark Dawson-Mau'u

4.Name of the Staff Member: s 9(2)(a)

5.Summary of the Investigation: On 22 September 2022 s 9(2)(a) had drinks with friends at the Trax Tavern at the Wellington Train Station, she left at 9:45pm and had also left her work bag which contained her IR issued laptop device. She did not realise until the next morning and contacted the Trax Tavern immediately who advised that it had not been handed in. She reported the loss to the Wellington Police and completed the IR internal process to ensure it was deactivated. Other contents in the laptop bag were her photo ID card and some ASPIRE training notes.

6.Summary of Enquiries: Initial enquiries were made with IA - Corporate Security (IR) who confirmed that they had visited the Trax Tavern and the device was able to be located and returned along with the bag and referenced contents. Conversations were then had with Murray Deadman (Substantive reporting line TL) who confirmed the timing of being notified of the incident from s 9(2)(a) on the Friday and then advising her of the steps that needed to be taken from her as well as notifying me. I was unable to meet with s 9(2)(a) immediately due to already scheduled external commitments and leave. I had an informal meeting with s 9(2)(a) on 8 November to gain an understand of what had occurred and why she had taken her device to venue in question. s 9(2)(a)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

7.Findings and Conclusions: s 9(2)(a)

[REDACTED] She ensured her TL was notified as soon as she became aware of the incident and has been remorseful throughout the process. Further she had proactively undertaken a refresher of the "Use of Business Tools" learning and provided her team colleagues with an integrity session. On 14 November I had another meeting with s 9(2)(a) regarding my findings and during this time she was even more apologetic and s 9(2)(a)

[REDACTED] On that basis I find that a verbal warning is sufficient

8.Final Status of Employee: s 9(2)(a)

9. Analysis of how incident occurred: s 9(2)(a)

There could have been a variety of other alternatives ie. leave the device at work, select another venue close to home etc however an accumulation of all the elements shared would have made these more challenging ie. s 9(2)(a) WFH the next day and the associated logistics / convenience

10. Incidental Findings: As shared

11. Recommendations: Integrity reminder to all that take IR devices home with annual refreshers on use of business tools

12. Outstanding Issues: Nil

13. Referral to Police: Nil

14. Protected Disclosure: Nil

15. I have forwarded all documentation to Integrity Assurance (Please destroy all other copies):
Yes

From: IR ServiceNow s 18(c)(i)
Sent: Wednesday, 17 May 2023 9:45 am
To: Tania McMullin s 9(2)(a); Ta'au Savaiinaea s 9(2)(a);
Integrity WIP s 18(c)(i); Chris Linton s 9(2)(a); Fune Parsons
s 9(2)(a); Nikora Conroy s 9(2)(a); Fiona Tuffery
s 9(2)(a)
Subject: [IMPORTANT] Sensitive incident task SENTSK0001111 has been assigned to your group
Importance: High



Inland Revenue
Te Tari Taake

----- This email address is not monitored -----

If you have a query about this ServiceNow ticket please raise an issue on the [Support Portal](#) or if you don't have access to ServiceNow call the IT Service Desk on 0800 474 843 opt.1

What you need to know:

Sensitive incident task [SENTSK0001111](#) has been assigned to your group **ASGN-Integrity**

This task was created as part of sensitive incident [SEN0001053](#)

Please review the task details and complete actions as applicable.

[Unsubscribe](#) | [Notification Preferences](#)

Ref:MSG14745693

Final Report received from Josh Green

Tuesday, June 20, 2023 12:19 PM

Case Number: 2023/078

Submitted by: Josh Green

Decision maker (if different from above):

Name of the employee under investigation: s 9(2)(a)

What was alleged or suspected?: s 9(2)(a) left her bag (including her laptop) on the bus

What actually happened?: s 9(2)(a) left her bag (including her laptop) on the bus. She remembered realised when she got off the bus, but it was too late. She attempted to contact the bus company to see if the bag and contents would be retrieved as soon as they opened the next day. It took about 3 days for the bag and device to be recovered.

How did it happen?: Human error

Where did it happen?: Karori bus

Final outcome for this employee: No Offence

Serious Misconduct established: No

Breach of S.18 established: No.

Outstanding actions or issues: I have had a conversation with the person

Recommendations: Remind people of the importance of keeping control of their possessions and keeping electronic versions of sensitive information (paper copies were not involved in this case, but it highlights the risk of paper versions)

Additional comments: I found the reporting form easy to use, but I think the replacement device thing would be worth putting some context around when a new device is required - I assumed there would be a stand down period before requesting a new device to see if it was recovered, but it would have been easier if I requested a new device immediately on the basis it would be wiped and recirculated

I have forwarded all original documentation / evidence obtained to Integrity and destroyed all other copies:["Yes"]

Appendix B

Initial report received from Karen Whitiskie

Tuesday, April 19, 2022 11:58 AM

- 1.Name of the person submitting the form: Karen Whitiskie
- 2.Name of the employee: s 9(2)(a)
- 3.Name of the employees manager: s 9(2)(a)
- 4.Employees Location: Wellington
- 5.Business Area: CCS- Business
- 6.Detection Type: Event Report
- 7.Previously disciplinary outcomes (include type, date and why): I am not aware of any.
- 8.Performance Issue?: No
- 9.Description of the issue: s 9(2)(a) transferred 10 audio files to a USB stick to take to Upper Hutt to have the Digital Forensic team transfer it to CD Rom to enable s 9(2)(a) then to be able to give criminal disclosure to a prisoner who IR is prosecuting. CD Rom is required given the person is in prison, it can't be via USB. The USB was in its original plastic container, with 3 post it's on it. One of the post its contained the password to access the USB which had been encrypted via Bitlocker. The USB was tucked in a eastlight which was wrapped with Green String. Somewhere between s 9(2)(a) desk and the end of the lane/driveway from Freyberg Building (where s 9(2)(a) car was parked) the USB is believed to been lost. A search of the office and the driveway has not located the USB.
- 10.How was the issue identified? (Give details): s 9(2) reported it to his Technical Lead who reported through the on-line reporting system.
- 11.Action taken to date: Dawn Swan and Catherine Lee were met with and following their advice a report was made to the Police.

Final report received from Karen Whitiskie

Tuesday, May 10, 2022 11:55 AM

1. Case Number: Case 2022/032

2. Email address for confirmation: s 9(2)(a)

3. Your Name: Karen Whitiskie

4. Name of the Staff Member: s 9(2)(a)

5. Summary of the Investigation: s 9(2)(a) reported the loss of the USB stick (which was encrypted by bitlocker but the password was on an attached post it note) to his Technical Lead and on her guidance logged a potential privacy breach report (on 13 April 2022). s 9(2)(a) met with Dawn Swan and Cathy Lee on 14 April and provided additional information. The USB is believed to have been lost somewhere between the 9th floor of Freyberg and s 9(2)(a) car which was parked across from the at the end of the access road to Freyberg. The USB was tucked into an eastlight folder which had been tied with green string. The USB was being transported to IR's Upper Hutt office for the 10 audio files of witness interviews to be burnt on to a CD Rom to be provided to a prison at s 18(c)(i) prison as part of the criminal discovery process as the USB could not be provided. They stopped first at the prison to drop off a folder for criminal discovery and at that point realised the USB was missing. A call to the office mistakenly caused them to believe the USB had been left on s 9(2)(a) desk but as soon as he returned to the office he realised it was the wrong USB. The USB was encrypted with bitlocker but one of the post it notes on the USB contained the password (but without reference to it being the password) and contact names and numbers of two correction officers was on another post it note. s 9(2)(a) (who had accompanied s 9(2)(a) on the trip) retraced their steps but were unable to locate the USB. The mailroom was advised but nothing had/has been handed in. As part of the discussions with Dawn Swan an all Freyberg communication was sent asking if anyone had found a USB to provide it to the mailroom and a lost property report was made to the police. The USB has not to date been located.

6. Summary of Enquiries: I have spoken with s 9(2)(a) several times to understand what happened, the steps he has taken to locate the missing USB and his actions in reporting it missing. I have also spoken to him about how the password came to be on the USB and its method of transport and what he considers he should have done differently. s 9(2)(a) has also assisted with working with the Crown Solicitor s 9(2)(h)

I have spoken with s 9(2)(a) s 9(2)(a) Technical Lead, several times. s 9(2)(a) confirms that s 9(2)(a) advised her what had happened and was very distressed about it when he spoke to her. She had located the privacy breach reporting tool for s 9(2)(a) to make the report. I also spoke with s 9(2)(a) who accompanied s 9(2)(a). She advised that s 9(2)(a) had made sure they had the USB with them and had been particularly conscious of it. s 9(2)(a) had gone to obtain a scan of the file and USB for their records before leaving and she does not recall if she saw the USB after that. When they arrived at s 18(c)(i) prison she had rung back to the office and talked with Tara Carr who had advised that a USB was sitting on s 9(2)(a) desk. On their return to the office when they realised it was the wrong USB (it was the copy for the Crown Solicitor), they had retraced their steps, searching for the USB and had searched s 9(2)(a) car. I have also followed up on whether s 9(2)(a) had a USB exemption. Legal Services had a bulk exemption (which included s 9(2)(a)) up until September 2021. In September last year Cyber Security changed the process and Team Leads were asked to submit a request on behalf

of all their team members. As s 9(2)(a) was still able to use a USB in his machine I believe he continued to have the necessary exemption but have not been able to get access to date to the relevant reports. I am working with Jay Harris on this. I understand that Jay will also be looking into how the USB exemption process works.

7. Findings and Conclusions: I am satisfied this was a one off accidental loss of a USB by s 9(2)(a) is genuinely upset and apologetic for what has happened. s 9(2)(a) appropriately encrypted the USB but I consider two mistakes were made, both of which s 9(2)(a) has acknowledged. Firstly, s 9(2)(a) should not have attached a post it note with the password to the USB. The password should have either been sent by email to Neville Winter for him to use in burning to CD Rom. Secondly, the folder should have been in a secure case for transportation. As this is a one off mistake by s 9(2)(a), which he promptly reported to his Technical Lead and followed instructions on the notification process and has taken follow up actions asked of him, I consider no employment action is required. My view would be different if such a mistake was to happen again in the future but given s 9(2)(a) genuine distress over what has happened and the steps that have had to be taken, I believe this mistake will not be repeated. As s 9(2)(a) s 9(2)(a) has continued to be able to use a USB in his computer and encrypt with bitlocker, it appears his leader renewed the necessary exemption for him or other steps were taken to continue the existing exemption he had prior to September last year. This will be confirmed when I have the necessary reports. Legal Services needs to work closely with Jay Harris and his team on any changes to the USB exemption process going forward.

8. Final Status of Employee: No Offence

9. Analysis of how incident occurred: The accidental loss of the USB is down to human error but the risk of the loss and the impact of the loss could have been avoided if two steps were taken. The password should not have been put on a post-it note on the USB - it should have been sent separately to the recipient. The file and USB should have been transported from the office in a secure case.

10. Incidental Findings: There have been a number of incidental findings from this incident. There will be separate work undertaken as to the IR incident management process for early escalation of such issues. Jay Harris is looking at what improvements can be made around the use, security and tracing of USB's and will be including some additional material on USB's in the revised security training being done. The Legal Services USB processes need updating to ensure it addresses both civil discovery and criminal disclosure processes and building and storage changes. The current processes focus on the use of USB's in civil procedures, and transportation to and from Crown Law. Given changes in personnel, further education within the team is required, it needs to be incorporated into our induction process and ongoing team education incorporated into the quarterly BMC process. Ross Walker advised that the CCS document transportation policy is out of date and needs to be revised. A organisation lesson learnt has been done and a report is currently being completed.

11. Recommendations: As per above, further organisation work will be undertaken by Jay Harris on the use, security and tracing of USB's which Legal Services will assist with. Legal Services Leaders will have a quarterly BMC check to undertaken in respect of the use of USB's. The CCS document transportation policy is out of date and needs to be updated but it was agreed as part of the incident management process that it should be an IR wide policy. I have asked Eteline Tiraa to work with Ross Walker to achieve this.

12. Outstanding Issues: The work on the Legal Services USB policy will be finalised this week -

Action point Eteline Tiraa. This policy will need to be further updated after Jay Harris completes the wider organisational work on the use of USB's - Action Point Eteline Tiraa BMC questions are being reviewed to identify how incorporate reporting on our USB policy into the quarterly process - Action point Eteline Tiraa and accountability each quarter with leaders completing BMC checks.

13.Referral to Police: N/A

14.Protected Disclosure: N/A

15.I have forwarded all documentation to Integrity Assurance (Please destroy all other copies):
Yes

From: [Cath Atkins](#)
To: [Karen Whitiskie](#)
Subject: RE: USB stick
Date: Thursday, 14 April 2022 3:59:28 pm
Attachments: [image001.png](#)
[image002.png](#)

Don't be sorry you are on leave! Your going to cancel this days leave soon.
It doesn't sound like we can do much at the moment, but do wonder what we need to tell folk at some stage if it doesn't turn up.

Noho ora mai

Cath Atkins([she/her](#))

Deputy Commissioner Customer & Compliance Services - Business | Inland Revenue Ratonga
Kiritaki Me te Tautukunga - Pakihi | Te Tari Taake

s 9(2)(a) PO Box 2198 | Wellington



From: Karen Whitiskie s 9(2)(a)

Sent: Thursday, 14 April 2022 3:58 pm

To: Cath Atkins s 9(2)(a)

Subject: RE: USB stick

Sorry no but I am getting across it now.

From: Cath Atkins s 9(2)(a)

Sent: Thursday, 14 April 2022 3:53 PM

To: Karen Whitiskie s 9(2)(a)

Subject: FW: USB stick

Nothing to do ... but I assume you are in the loop on this?

Noho ora mai

Cath Atkins([she/her](#))

Deputy Commissioner Customer & Compliance Services - Business | Inland Revenue Ratonga
Kiritaki Me te Tautukunga - Pakihi | Te Tari Taake

s 9(2)(a) PO Box 2198 | Wellington



From: Dawn Swan s 9(2)(a)

Sent: Thursday, 14 April 2022 3:28 pm

To: Mary Craig s 9(2)(a); Cath Atkins s 9(2)(a)

Subject: USB stick

Hi Mary and Cath

No need to panic but just thought I'd give you a heads up that one of our solicitors has lost a USB stick. While the USB is encrypted, it had a post-it note attached that contained the password.

The USB got lost either inside the Freyberg building (level 9 or lower ground floor), in the service lane or in the staff member's car. The staff member had been parked about

70m away from the Freyberg entrance on the service lane. All areas have been checked but it hasn't been located. I've asked the coms team if we can send an email out to all Freyberg users just in case someone has picked it up but didn't know what to do with it. The USB contains audio files of interviews with s 18(c)(i) (who we are currently prosecuting) and 9 witnesses. It was lost on Tuesday and got notified yesterday, I've informed the media team and it's been reported to the Police. We've done all we can for now but because we haven't been able to locate the USB there is an ongoing risk that someone may have picked it up.

Dawn Swan

Privacy Officer | Enterprise Design & Integrity | Inland Revenue

Asteron Centre, 55 Featherston Street, Wellington

PO Box 2198, Wellington 6140



[Call/chat with me in Teams](#) s 9(2)(a)

From: [Eteline Tiraa](#)
To: [Legal Services - Wider Leadership Team](#)
Subject: Friendly reminder re Privacy Breaches
Date: Tuesday, 19 April 2022 12:19:59 pm

Hi,

Just a friendly reminder that for any privacy breach you or someone in our team may need to report if you could also let Karen and myself (and your reporting Domain Lead) know in the first instance. This helps to ensure we can effectively manage other channels promptly particularly where there may be strong media interest, etc. and support/manage expectation of what this may mean for others in IR including our Commissioner.

As always, there is information on our intranet: [Privacy breaches \(sharepoint.com\)](#) and the process to follow when needing to lodge such incident(s).

Some of you may be aware of the comms sent out to all Freyberg users last week re a missing USB but we ask that we do not discuss this further while we work through the incident that has been reported.

Hope you all enjoyed and had a relaxing Easter weekend

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

s 9(2)(a)



From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: FW: Missing USB
Date: Tuesday, 19 April 2022 9:57:18 am
Attachments: [v535xeom.0by.pdf](#)

From: s 9(2)(a)
Sent: Thursday, 14 April 2022 2:27 pm
To: Dawn Swan ; Catherine Lee ; Gay Cavill
Subject: Missing USB

Hi Dawn, Catherine,
As discussed

s 9(2)(a)


s 18(c)(i)

2)(a)

Recordings

ADATA
UV150 / 32GB

s 9(2)(h)



From: [Jay Harris](#)
To: [Karen Whitiskie](#)
Subject: FW: s 18(c)(i) Disclosure
Date: Tuesday, 19 April 2022 1:31:14 pm
Attachments: [Advance hunting USB.xlsx](#)

Hi....

I asked the SecOps team to validate that the 2nd USB was made and transmitted....See the response below, but unless s 9(2)(a) had someone else make the 2nd (or 1st) copy to the USB, SecOps can only see it being done once?

Let's discuss.

Jay

From: Ash Pathan
Sent: Tuesday, 19 April 2022 1:23 PM
To: Jay Harris
Subject: RE: s 18(c)(i) Disclosure

Hi Jay,

I can confirm from the logs that s 9(2)(a) never made a second copy of the USB. His computer logs show only 1 usb drive with serial number AA00000000000489 was used for data copy. However the same drive is used by Andrew McClusky to copy following files.

s 18(c)(i)

The USB drive does not appear to be used for data storage after Andrew McClusky used.

The last person to use the Same USB is Jason Deng who used the USB drive on IR network on 2 days ago for data read.

In summary. I am certain s 9(2)(a) did not make 2 copies of USB. There is only one drive he used. After his usage there are 2 other users who were in possession of the same USB drive with last person to use is Jason.

Thanks,

Ash

Ash Pathan | Cyber Security Technology Specialist | Tiger Team (Threat Intelligence Gathering & Event Response) | Inland Revenue

s 9(2)(a)

From: Ash Pathan
Sent: Tuesday, 19 April 2022 12:27 pm
To: Jay Harris s 9(2)(a)
Subject: RE: s 18(c)(i) Disclosure

Hi Jay,

I can confirm that user has Bitlocker permission for USB file copy. He is given the permission via dedicated policy. PFA attached report of files copied by the user in question.

The transcript files that are copied are temporary files and may/may not contain all the information. Files being temporary they are hidden for normal user session. However any other PDF document and excel spreadsheet is readable.

Unfortunately If user has attached/provided the bitlocker password to the drive we cannot remotely revoke it.

Thanks,

Ash

Ash Pathan | Cyber Security Technology Specialist | Tiger Team (Threat Intelligence Gathering & Event Response) | Inland Revenue

s 9(2)(a)

From: Jay Harris s 9(2)(a)

Sent: Tuesday, 19 April 2022 11:50 am

To: Ash Pathan s 9(2)(a)

Subject: FW: s 18(c)(i) Disclosure

Hi...some more info below.

Jay

From: Karen Whitiskie s 9(2)(a)

Sent: Tuesday, 19 April 2022 11:49 AM

To: Jay Harris s 9(2)(a)

Subject: FW: s 18(c)(i) Disclosure

Hi Jay

s 9(2)(a) did the saving of 10 audio files to the USB last Tuesday morning. They came from the path below. s 9(2)(a) advises me that he used bitlocker for the encryption.

Let me know if you need any other information or need to speak with s 9(2)(a)

Thanks

Karen

From: s 9(2)(a)

Sent: Tuesday, 19 April 2022 11:46 AM

To: Karen Whitiskie s 9(2)(a)

Subject: s 18(c)(i) Disclosure

s 18(c)(i)

s 9(2)(a)

From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: Usb
Date: Tuesday, 19 April 2022 9:01:26 am

Hi Karen,

Teams stopped working for me. I don't have access to any details and of the incident or a copy of the report s 9(2)(a) submitted.

s 9(2)(a) called me as soon as he realized the USB was missing. He had it in a packet with a post it note with the password and name and phone number of the prison officer he was meeting at s 18(c)(i) prison to hand over the disclosure. USB was tucked into the inside cover of the file with a green string around it. No briefcase, just carried the file from desk to car. Arrived at s 18(c)(i) and USB gone. Missing between his desk and prison. Car was parked outside Freyberg so close proximity but could be lost inside the office, in the lift or on street between building and his car, or in car.

Iv had no update since the incident.

s 9(2)(a)
Get [Outlook for Android](#)

From: [Vanessa Johnson](#)
To: [Joanne Petrie](#); [Jay Harris](#); [Josh Green](#); [Rowan McArthur](#); [Ta'au Savaiinaea](#); [Karen Whitiskie](#); [Kirsty Gemmill](#)
Cc: s 9(2)(a)
Subject: RE: Lost USB Incident
Date: Tuesday, 19 April 2022 9:35:22 am

Hi Everyone

Can I suggest we work through the following framework to make sure we are all up to speed:

What do we already know

What do we need to know

Who do we need to tell

Who needs to do what by when

Vanessa

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue

s 9(2)(a)

-----Original Appointment-----

From: Joanne Petrie

Sent: Tuesday, 19 April 2022 8:41 AM

To: Joanne Petrie; Vanessa Johnson; Jay Harris; Josh Green; Rowan McArthur; Ta'au Savaiinaea; Karen Whitiskie; Kirsty Gemmill

Cc: s 9(2)(a)


Subject: Lost USB Incident

When: Tuesday, 19 April 2022 10:30 AM-11:00 AM (UTC+12:00) Auckland, Wellington.

Where: Microsoft Teams Meeting

Morena – Naomi and Mary have asked a team to come together to understand where this incident is at, the plan going forward and possible implications etc. Can you please make this a priority meeting – thank you!

Not in scope



From: [Ta'au Savaiinaea](#)
To: [Karen Whitiskie](#)
Subject: Initial Report Link
Date: Tuesday, 19 April 2022 11:20:04 am

Hi Karen

Initial Report Link - s 18(c)(i)

Regards

Ta'au

Ta'au Savaiinaea | Domain Specialist (L2) | Integrity and Internal Assurance

Enterprise Design and Integrity (ED&I) | INLAND REVENUE

s 9(2)(a) | www.ird.govt.nz

o PUTTING INTEGRITY FIRST – TU KI TE PONO o

From: [Joanne Petrie](#)
To: [Vanessa Johnson](#); [Karen Whitiskie](#); [Jay Harris](#); [Kirsty Gemmill](#); [Josh Green](#); [Rowan McArthur](#); [Ta"au Savaiinaea](#)
Cc: [Naomi Ferguson](#); [Dawn Swan](#)
Subject: Meeting Notes - Lost USB Incident - 19 April
Date: Tuesday, 19 April 2022 3:47:31 pm
Attachments: [Meeting Notes - Lost USB Incident - 19 April.docx](#)

Kia ora

Please find attached the notes from this morning's meeting in relation to this incident.

I will see you all online again at the follow up meeting tomorrow, Wednesday 20 April at 2pm.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

Lost USB Incident
Meeting: Tuesday 19 April 2022, 10.30am-11am

Attendees:

Vanessa Johnson (Lead)
Karen Whitiskie
Jay Harris
Kirsty Gemmill
Josh Green
Rowan McArthur
Ta'au Savaiinaea
Jo Petrie

What we know/factual information:

A staff member within Legal Services was transporting a USB key out to the Upper Hutt Office to have it saved onto a CD-ROM. This format is required to be accepted by s 18(c)(i) Prison. The Prison does not accept USB Sticks. The USB Stick held interviews with 10 people for a current prosecution case IR is taking and we were providing that as part of disclosure to the person we are prosecuting. The USB Stick was within a plastic container, tucked inside a Eastlight file and was tied up with string.

The USB Stick is thought to have been lost either within FRY building or surrounds or in the individual's car. The staff member went from FRY down to the Lower Ground and to his car at the end of the driveway. He went to the prison to drop off the Eastlight file before going to Upper Hutt to get the USB contents transferred to the CD-ROM. He realised that the USB Stick was missing. He phoned the FRY Office and a USB Stick was located on his desk. He assumed this was the missing USB. On return to the Office he realised it was not the missing USB stick.

An Incident Report was lodged on Wednesday morning (13 April 2022). He also talked to the mailroom at Upper Hutt to check if they had seen it – no one had.

A Post Note was attached to the USB Stick which was lost with the password on it. It also had x2 names and phone numbers in relation to the contacts at the prison that the staff member could phone if he had any issues getting into the prison. The password was also written on the Post-it Note - numbers and digits. The word 'password' was not written on it.

The staff member's Technical Lead went online to see what to do – reported it on Incident Management on the intranet – this report went to Dawn Swan and Catherine Lee – Catherine Lee advised the Technical Lead that the staff member should advise the Police. The staff member did this and made a Police report last week.

Jay Harris confirmed that an individual security exemption was not granted for the USB. Karen advised that Legal Services has general admin access/a broad exemption but had understood this process was updated but advised that the staff member didn't follow the updated process.

This prosecution is an active prosecution against a s 18(c)(i) The individual has not yet been advised.

Actions Taken:

Dawn Swan advised on 14 April 2022 that a privacy assessment had been made and it was not necessary to advise those interviewed of this.

Actions to be Taken:

s 9(2)(h)

Action: Karen Whitiskie

- 2 Organise for Cyber Ops to check if USB Stick has been accessed on an IR Device post the last access by the staff member on Tuesday 12 April.

Action: Jay Harris

- 3 Privacy assessment to be made as appropriate as this progresses.

Action: Karen/Dawn

- 4 Ta'au to send link to Karen to open an integrity case (including covering off if staff member had completed security modules as required).

Action: Ta'au Savaiinea

- 5 Consider scenarios we might need to deal with from a media perspective – both IR and Minister.

Action: Rowan

- 6 Contact Business Incidents (Catherine Lee/Manager) to understand what has been completed, how this was managed, what has been done or being done. The process for managing incidents that are reported via this system.

Action: Jo Petrie

Actions Moving Forward:

- 6 Education - Consider how we manage these processes – provide confidence to the public in relation to how we manage information generally. Also consideration with these instances vis a vis the email sent to all FRY staff disclosing that the USB Stick had been lost.

Action: Jay Harris

Next Meeting to be scheduled Wed afternoon (Jo Petrie to action)

From: [Ta'au Savaiinaea](#)
To: [Karen Whitiskie](#)
Subject: Final Report - Case 2022/032
Date: Wednesday, 20 April 2022 2:58:05 pm

[UNCLASSIFIED]

Hi Karen

As discussed, you should be satisfied that the actions taken in the recent breach of privacy by staff member s 9(2)(a) were accidental and that there is no evidence to support further action, in this instance.

If you consider the matter does not warrant further formal action, please confirm the basis for your conclusion by furnishing a FINAL REPORT (quote case 2022/032). **Please note that this is not a notification to commence an employment investigation.**

Furnishing the FINAL REPORT will close the matter and no further action will be required by you. Final report link - s 18(c)(i)

Should you have any questions regarding this email, please contact me by email or teams
Kind Regards

Ta'au

Ta'au Savaiinaea | Domain Specialist (L2) | Integrity and Internal Assurance
Enterprise Design and Integrity (ED&I) | INLAND REVENUE

s 9(2)(a) | www.ird.govt.nz

o PUTTING INTEGRITY FIRST – TU KI TE PONO o


From: [Karen Whitiskie](#)
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: Query
Date: Wednesday, 20 April 2022 10:33:52 am

Hi s 9(2)(a)

Two things

Firstly, is there any transcripts of the 10 audio files as opposed to listening to the recordings?

s 9(2)(h)





Ngā mihi

Karen Whitiskie (*she/her*)

Legal Services Leader | Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)



From: [Jay Harris](#)
To: [Karen Whitiskie](#)
Subject: RE: "Duplicate" USB
Date: Wednesday, 20 April 2022 3:09:34 pm

Thanks Karen

Hope you have a relaxing weekend with some excellent wine!

Jay

From: Karen Whitiskie
Sent: Wednesday, 20 April 2022 2:35 PM
To: Jay Harris
Subject: "Duplicate" USB

Hi Jay

I have given the USB to Rhys Brown from my team as he is in the office each day for the rest of the week.

The password is s 18(c)(i)

Ngā mihi

Karen Whitiskie (*she/her*)

Legal Services Leader | Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: s 9(2)(a)
Sent: Wednesday, 20 April 2022 2:44 pm
To: Karen Whitiskie
Cc: s 9(2)(a)
Subject: RE: Query

Hi Karen, s 9(2)(a)

We do have transcripts,

s 9(2)(h)

Regards,

From: Karen Whitiskie
Sent: Wednesday, 20 April 2022 10:34 am
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: Query

Hi s 9(2)(a)

Two things

Firstly, is there any transcripts of the 10 audio files as opposed to listening to the recordings?

s 9(2)(h)

Ngā mihi

Karen Whitiskie (*she/her*)
Legal Services Leader | Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'
s 9(2)(a)

From: [Joanne Petrie](#)
To: [Vanessa Johnson](#); [Jay Harris](#); [Karen Whitiskie](#); [Ta"au Savaiinaea](#); [Rowan McArthur](#); [Josh Green](#); [Kirsty Gemmill](#); [Dawn Swan](#)
Cc: [Naomi Ferguson](#)
Subject: Meeting Notes - Lost USB Incident - 26 April
Date: Friday, 22 April 2022 11:45:05 am
Attachments: [Meeting Notes - Lost USB Incident - 26 April.docx](#)

Kia ora koutou

Please find attached the notes from Wednesday's meeting. I have sent an appointment for the next update on Tuesday 26 April as well as an appointment for a Lessons Learned session in May.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

Lost USB Incident
Meeting: Tuesday 26 April 2022, 2.30pm-3pm

Attendees:

Vanessa Johnson (Lead)
Karen Whitiskie
Jay Harris
Kirsty Gemmill
Josh Green
Gay Cavill
Ta'au Savaiinaea
Jo Petrie
Dawn Swan

Open Action Points

Action Point 1 – Karen – s 9(2)(h)

No update at this stage.

Reference to Privacy Assessment of Corrections staff

Dawn: two names were names of Correction Staff – staff member was going to advise corrections officers and let them know. Karen advised staff member didn't do this but will check in with them.

Action Point 2 – Jay Harris – USB Stick

Talked to s 9(2)(a), there were four USB keys, they were all used at the same time, Jay has validated that. The one we are questioning is the one missing. They still have no evidence of multiple USB sticks being plugged into machines. This will be part of lessons learned. We have a gap in our log management. Three in our possession. Jay still to get duplicate from Legal Services as per earlier action point.

Confirmed that the key is lost/not in our possession. Karen to work through s 9(2)(h) – hasn't hit any media or social media as far as we know.

Jay ultimately would like all three USB sticks to understand what can be seen or not.

MOVE TO LESSONS LEARNED

Action Point 5 – Rowan/Josh – Media/Minister

Watching Briefing continues.

s 9(2)(h)

Action point to continue to be open

Action Point 6 – Jo Petrie – Contact Business Incident

CAN BE CLOSED – feed into lessons learned – how was made aware.

Action Point 8: Jay to contact Neville Winter to understand his actions in relation to the USB Stick access (it was confirmed he used a system 'off the grid' – need to incorporate this into lessons learned conversation).

Jay spoke with s 9(2)(a) to follow up.

Action Point 9: Karen to advise Jay who has the other USB stick so then Jay can contact them, identify it and confirm.
ACTION POINT CAN BE CLOSED

Action Point 10: Jay will prepare a visual timeline of names they are seeing who accessed the USB stick and provide that to the Group.

Leave open and to be provided at a high level.

The names associated with USBs post s 9(2)(a) not confident around this information. Shows gaps in the process.

Action Point 11: Karen to ask the staff member to contact Jay to tease out the timing of what he did what/when. Can then validate that with logs.

This has occurred
ACTION POINT TO BE CLOSED

Updates:

Confirmed that the primary USB that had the voice files on is missing. Best case it got dropped and was destroyed. Not heard anything in media or social media. Still a holding pattern.

Ta'au has the internal aspect in hand. Will go through its process. Could be a cross over depending on what happens with lessons learned.

Lessons Learned to be brought forward to next week. Jo/Vanessa: Write up the front end of what happened, this is what we've done, and then the lessons learned out of that.

Josh: what is the Court timeline in terms of when we may disclose to the person of this.
s 18(c)(i)

Next Monday catch up again for the s 9(2)(h)

Lost USB Incident
Meeting: Tuesday 26 April 2022, 2.30pm

Attendees:

Vanessa Johnson (Lead)
Karen Whitiskie
Jay Harris
Kirsty Gemmill
Josh Green
Rowan McArthur & Gay Cavill
Ta'au Savaiinaea
Jo Petrie

Action Point Updates

Action Point 1 – Karen

The sub-Action Point: "Consider the privacy aspect for the two names listed on the Post-it Note" is to be transferred from Karen Whitiskie to Dawn to assess. Jo will ensure Dawn receives a copy of both sets of notes and will ask her to make this assessment and report back to the group.

s 9(2)(h)

She also confirmed she would get further clarity on the USB stick access etc.

Action Point 2 - Jay Harris - USB Stick

The access logs have been checked on both USB Sticks. However, the Cyber Ops Team can only find one USB key that the files have been copied to. The same USB stick was accessed/used on 4, 12 and 14 April. There is no evidence that there was another USB that was plugged into the machine at Digital Forensics.

Karen advised that it was Neville Winter who transferred the data, however, this was not appearing on the Cyber Ops log. It was noted that Neville Winter's machine may not appear 'on the log' given his role. The staff member was not contactable so Karen was unable to clarify the USB keys/access/duplicates etc.

There was confusion around the USB sticks, who, how many, what has been accessed etc and it was agreed there needs to be clarity provided.

New Action Point 8: Jay to contact Neville Winter to understand his actions.

New Action Point 9: Karen to advise Jay who has the other USB stick so then Jay can contact them, identify it and confirm.

New Action Point 10: Jay will prepare a visual timeline of names they are seeing who accessed the USB stick and provide that to the Group.

New Action Point 11: Karen to ask the staff member to contact Jay to tease out the timing of what he did what/when. Can then validate that with logs.

Action Point 4 – Ta'au – Employment Investigation (CLOSED)

A case has been opened. This Action Point can now be closed.

Action Point 5 – Rowan/Josh – Media/Minister

Still thinking if this becomes a story then a s18 exemption would be sought so we can effectively protect the integrity of the tax system. s 9(2)(h)

s 9(2)(h)

It was agreed we would be in a similar position with any briefings to the Minister in relation to this also.

Action Point 6 – Jo Petrie – Contact Business Incident

The following was confirmed by James Barker/Catherine Lee:

- The incident was raised by Cathy on Thursday 14 April and she discussed it with Dawn Swan.
- It was confirmed by Cathie that this incident was only managed from a 'privacy breach' perspective.
- Dawn assessed the privacy risk of those witnesses' interviews on the USB Stick and deemed it low risk given the staff member advised it was probably lost within the Freyberg building.
- Dawn arranged for an email to be sent to all Freyberg staff to "keep a eye out for the USB" as it was determined that the building was the most likely place that it was lost.
- Cathy has updated the ticket with the information from her conversation with Dawn
- Cathy confirmed that an email was sent to the staff member asking if the loss of the USB stick had been reported to the Police.
- I asked Cathy to send that email to Ta'au as he was covering this from an employee integrity perspective.

Next Steps

A meeting to be scheduled for Tuesday 26 April. If anything happens before then text Vanessa who will be annual leave but is contactable.

Schedule a lessons learned which should include Cathy Lee and James Barker as well as this Group in the first/second week of May.

From: s 9(2)(a)
Sent: Tuesday, 26 April 2022 10:56 am
To: Karen Whitiskie; s 9(2)(a)
Subject: RE: Query

Hi Karen,

s 9(2)(h)

Yours sincerely,

s 9(2)(a)

Technical Lead - Kaihautū ā-hangarau | Solicitor - Rōia
Legal Services – Ratonga Ture
Inland Revenue – Te Tari Taake
s 9(2)(a)

From: Karen Whitiskie
Sent: Tuesday, 26 April 2022 10:44 AM
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: RE: Query

Hi

Any chance of an update on this?

I have an update meeting on the missing USB later today.

Thanks

Karen

Not in scope

From: s 9(2)(a)
Sent: Tuesday, 26 April 2022 3:37 pm
To: Karen Whitiskie
Subject: RE: Follow up

Hi Karen,

I have just spoken to Dawn.

She is of the view that as we didn't do it right away it is probably better not to do it now. (given two weeks have passed)

I took Dawn to mean that raising it now would probably do more harm than good.

Regards,

s 9(2)(a)

From: Karen Whitiskie
Sent: Tuesday, 26 April 2022 3:13 pm
To: s 9(2)(a)
Subject: RE: Follow up

Hi s 9(2)(a)

Can you please call Dawn Swan about contacting the Corrections staff and let me know what advice she gives you?

Thanks

Karen

From: s 9(2)(a)
Sent: Tuesday, 26 April 2022 3:10 PM
To: Karen Whitiskie s 9(2)(a)
Subject: RE: Follow up

Hi Karen,

See below in red:

Regards,

s 9(2)(a)

From: Karen Whitiskie s 9(2)(a)
Sent: Tuesday, 26 April 2022 3:00 pm
To: s 9(2)(a)
Cc: s 9(2)(a) s 9(2)(a)
Subject: Follow up
Importance: High

Hi s 9(2)(a)

A few things:

- Have you contacted the two Corrections individuals that names and numbers were on missing USB? Dawn Swan seems to think you were going to but I wasn't aware that was the case. Can you clarify? **I suggested this, but I also raised a concern about disclosing this to the two individuals, I haven't been able to get a clear answer on whether this was appropriate, but I am happy to do it.**
- Can you please ensure we have the s 9(2)(h) **Yes, will do**
Can I please have a time line for the coming dates on the s 18(c)(i) prosecution? s 18(c)(i)
- Also s 9(2)(a) I will set up a meeting to discuss what has happened this week as we need to talk it through ahead of the lessons learnt I will be attending on this matter. **Noted**

Thanks

Karen

From: s 9(2)(a)
Sent: Tuesday, 26 April 2022 12:36 PM
To: s 9(2)(a) s 9(2)(a); Karen Whitiskie s 9(2)(a)
Subject: RE: Query

Hi there,


I have been down to the mailroom this morning and they have had nothing handed in to date.

No other updates at this stage

Not in scope, Duplicate



s 9(2)(a)





From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: FW: s 18(c)(i)
Date: Thursday, 28 April 2022 6:43:11 pm
Attachments: [image001.jpg](#)
[image002.jpg](#)
[image003.jpg](#)
[image004.jpg](#)
s 9(2)(a)





Hi Karen
s 18(c)(i)

Regards,
s 9(2)(a)

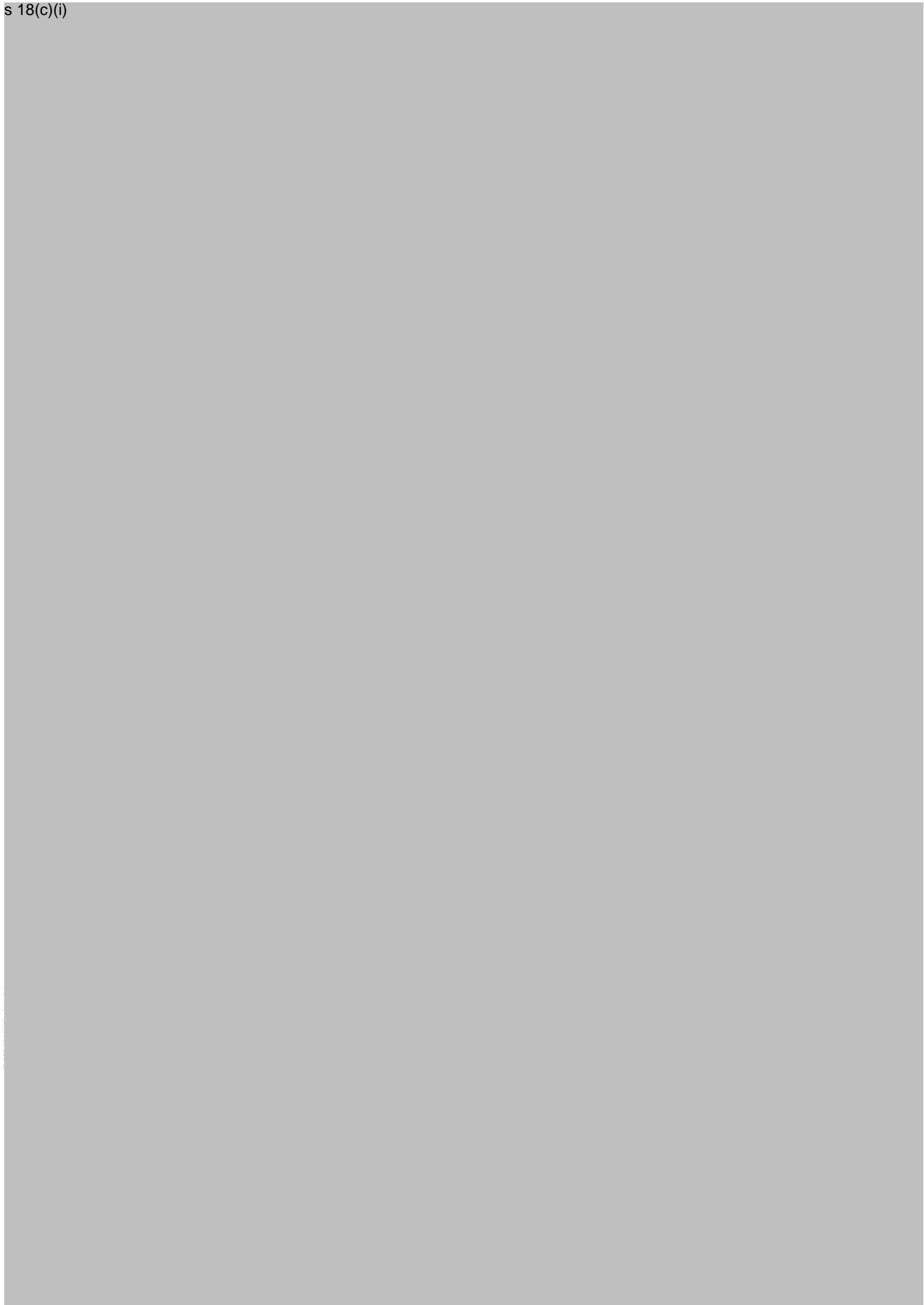
From: s 9(2)(a)
Sent: Wednesday, 20 April 2022 9:54 am
To: s 9(2)(a)
Subject: s 18(c)(i)

External Email CAUTION: Please take **CARE** when opening any links or attachments.

Hi
Document from s 18(c)(i)
Thanks
s 9(2)(a)
Department of Corrections Ara Poutama Aotearoa
s 18(c)(i)
s 9(2)(a)

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
|  |  |  |  |

The information in this message is the property of the New Zealand Department of Corrections. It is intended only for the person or entity to which it is addressed and may contain privileged or in confidence material. Any review, storage, copying, editing, summarising, transmission, retransmission, dissemination or other use of, by any means, in whole or part, or taking any action in reliance upon, this information by persons or entities other than intended recipient are prohibited. If you received this in error, please contact the sender and delete the material from all computers.



From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: FW:s 18(c)(i) Response
Date: Thursday, 28 April 2022 6:42:07 pm
Attachments: [image001.png](#)
[harristr1_13-04-2022_11-27-44.pdf](#)

Hi Karen,

I just sent you the lost property claim I made at Wellington Central Police station.

s 18(c)(i)

[Redacted]

[Redacted]

[Redacted]

Regards,

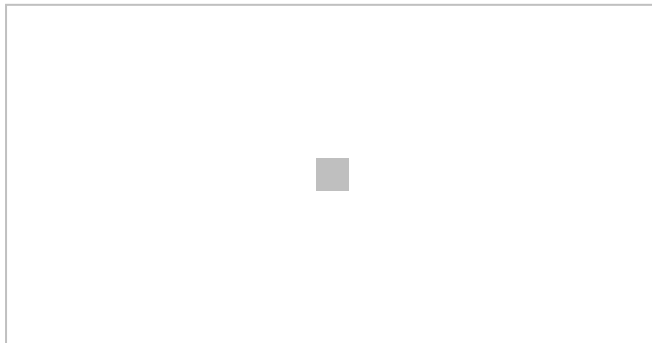
From: s 9(2)(a)
Sent: Wednesday, 13 April 2022 11:38 am
To: s 9(2)(a)
Subject: s 18(c)(i) Response

External Email CAUTION: Please take **CARE** when opening any links or attachments.

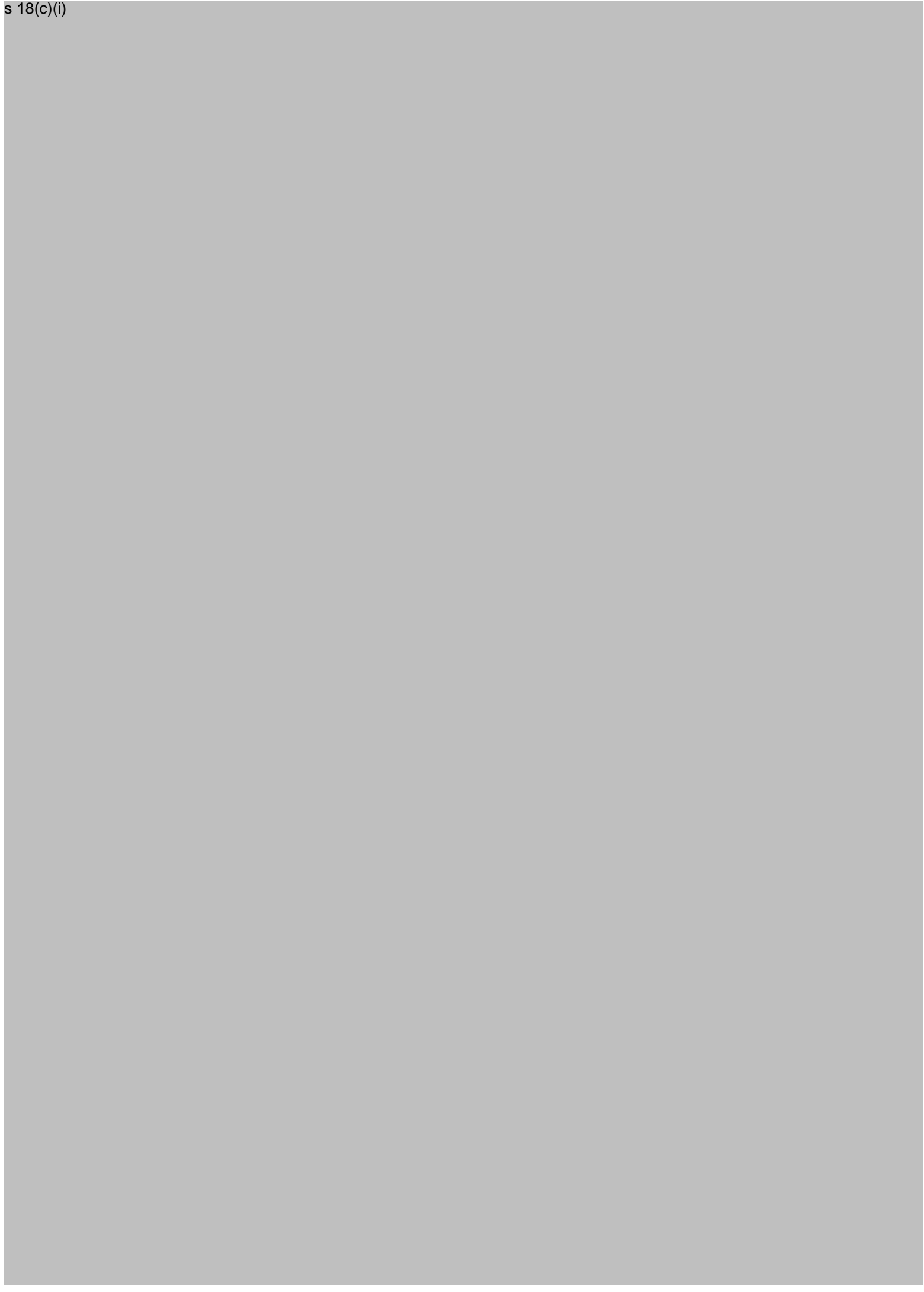
Good morning

Response to applications for in court media coverage attached.

Thanks

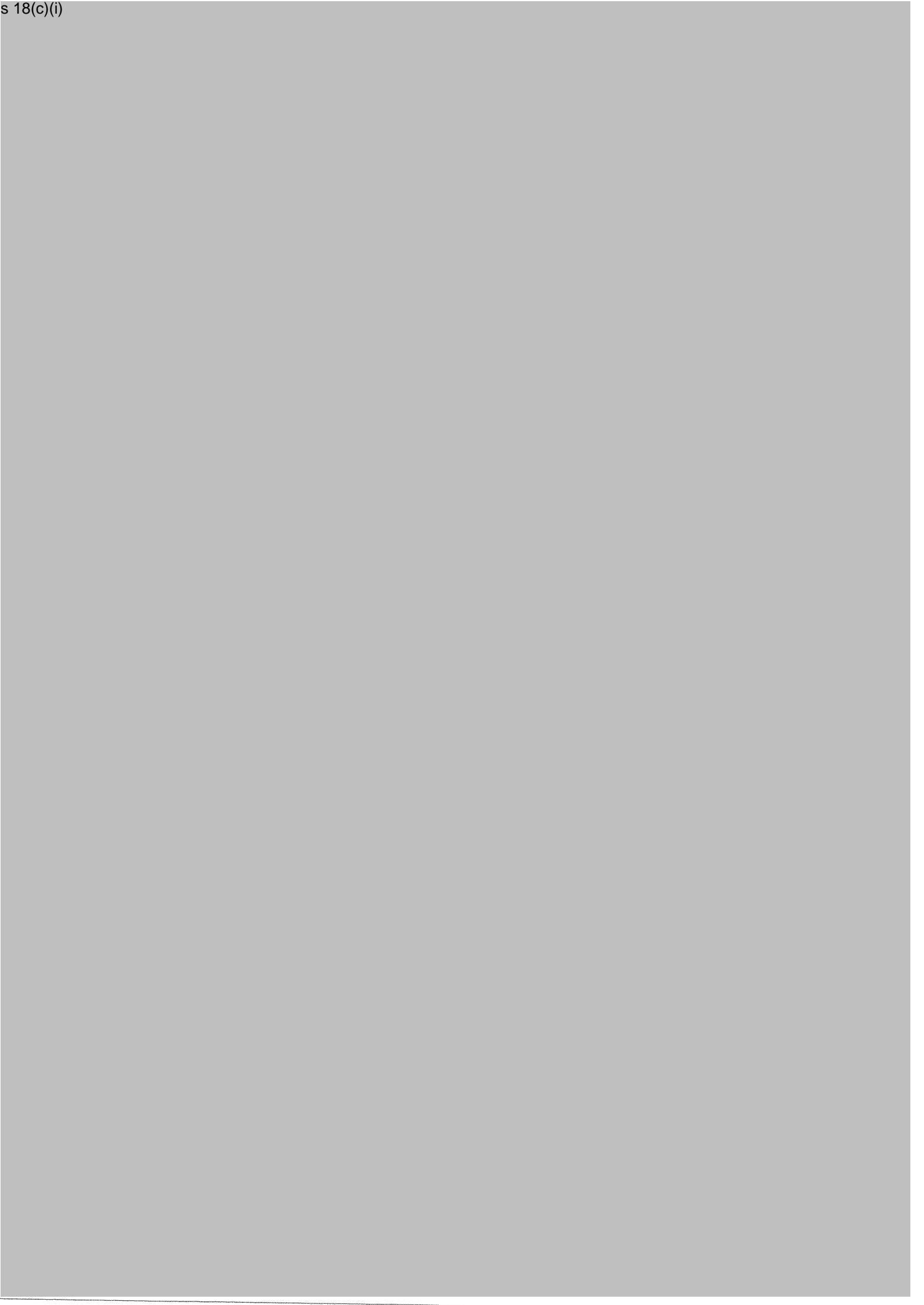


The information in this message is the property of the New Zealand Department of Corrections. It is intended only for the person or entity to which it is addressed and may contain privileged or in confidence material. Any review, storage, copying, editing, summarising, transmission, retransmission, dissemination or other use of, by any means, in whole or part, or taking any action in reliance upon, this information by persons or entities other than intended recipient are prohibited. If you received this in error, please contact the sender and delete the material from all computers.









From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: FW: Police Acknowledgement Form (File Ref: 220413/8149)
Date: Thursday, 28 April 2022 6:34:11 pm
Attachments: [PAF_REQUEST_FOR_s 9\(2\)\(a\).pdf](#)

[IN CONFIDENCE]

From: Wellington.FMC@police.govt.nz
Sent: Wednesday, 13 April 2022 4:52 pm
To: s 9(2)(a)
Subject: Police Acknowledgement Form (File Ref: 220413/8149)

External Email CAUTION: Please take **CARE** when opening any links or attachments.

“Do not reply to this message. This message has been sent from an unmonitored email address.”

Dear s 9(2)(a)

Please find attached a copy of your Police Acknowledgement Form with regards to the report you made to the **Wellington Central** police station on **13/04/2022 16:46:00**.

If you have any questions, comments, or would like to add anything to your report, please quote the reference number provided.

For further crime prevention information please visit Neighbourhood Support New Zealand's website <https://www.neighbourhoodsupport.co.nz/tips-advice>

For further information on recording of serial numbers and reducing offending please visit <http://www.snap.org.nz>.

To upload photos or documents relevant to your complaint, please visit <http://www.crl.govt.nz>.

Thank you,

Wellington Central Police

“Do not reply to this message. This message has been sent from an unmonitored email address.”(See attached file: *PAF_REQUEST_FOR_s 9(2)(a).pdf*)

WARNING

The information contained in this email message is intended for the addressee only and may contain privileged information. It may also be subject to the provisions of section 50 of the Policing Act 2008, which creates an offence to have unlawful possession of Police property. If you are not the intended recipient of this message or have received this message in error, you must not peruse, use, distribute or copy this message or any of its contents.

Also note, the views expressed in this message may not necessarily reflect those of the New Zealand Police. If you have received this message in error, please email or telephone the sender immediately

s 9(2)(a)

Police Acknowledgement

Details

Name: s 9(2)(a)

Address: s 9(2)(a)

Offence/Incident: Lost Property

Location: AITKEN STREET, THORNDON, WELLINGTON CITY

Date Reported: 13/04/2022 4:46 PM

Reference Number: 220413/8149

Description: 1 x ADATA UV150/32GB usb drive containing data. Retail value \$20nzd.

Please Note

To upload relevant photos or documents, please visit 105.police.govt.nz

If you need to speak to Police again on this matter please quote the reference number recorded above.

For insurance purposes a telephone report of crime is not evidence in itself that a crime has occurred.



USE 105 FOR POLICE NON-EMERGENCIES

CALL 111 FOR EMERGENCIES

Property and Belongings

Property crime can have a devastating impact. Here are some simple steps you can take to make your home and property as safe as possible:

1

Always lock your car, motorbike, bicycle or other vehicles. A car alarm, steering lock, or good quality chains are extra deterrents too. Ideally keep all vehicles in a garage or out of sight.

2

When out and about, keep your belongings secure and close to you. Separate your house and car keys, especially if you have an address on the key ring.

3

Don't provide places for burglars to hide — keep bushes and trees trimmed.

4

Don't answer the door for someone you don't know or don't want in your home. Ask for identification if they say they represent a company. If you're outside for an extended time, e.g. in the garden, lock your front door.

5

Keep valuables out of sight — If it can be seen, it can be a target. Keep receipts, warranties, valuations, and serial numbers in a safe place. Take photos or videos of jewellery, art and other precious items.

6

Secure your doors, windows, sheds and garages with good quality locks. Install security stays on windows, especially those on ground level.

From: [Rhys Brown](#)
To: [Karen Whitiskie](#)
Subject: USB drive
Date: Thursday, 28 April 2022 9:05:38 am

Hi Karen,
I still have the USB drive you left with me for safekeeping – nobody has asked for it. Did you want it back?
Rhys

From: [Joanne Petrie](#)
To: [Vanessa Johnson](#); [Karen Whitiskie](#); [Josh Green](#); [Conrad Bace](#); [Gay Cavill](#); [Jay Harris](#); [Dawn Swan](#)
Cc: [Kirsty Gemmill](#); [Naomi Ferguson](#); [Mary Craig](#)
Subject: Latest Updates
Date: Thursday, 28 April 2022 3:50:23 pm
Attachments: [Meeting Notes - Lost USB Incident - 26 April Notes.docx](#)
[Meeting Notes - Lost USB Incident - 28 April 2022.docx](#)

Kia ora koutou

Thank you again for meeting today at such short notice.

Please find attached the notes from our two meetings this week. I will also now schedule a further meeting for next Monday.

Any queries or changes please let me know.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

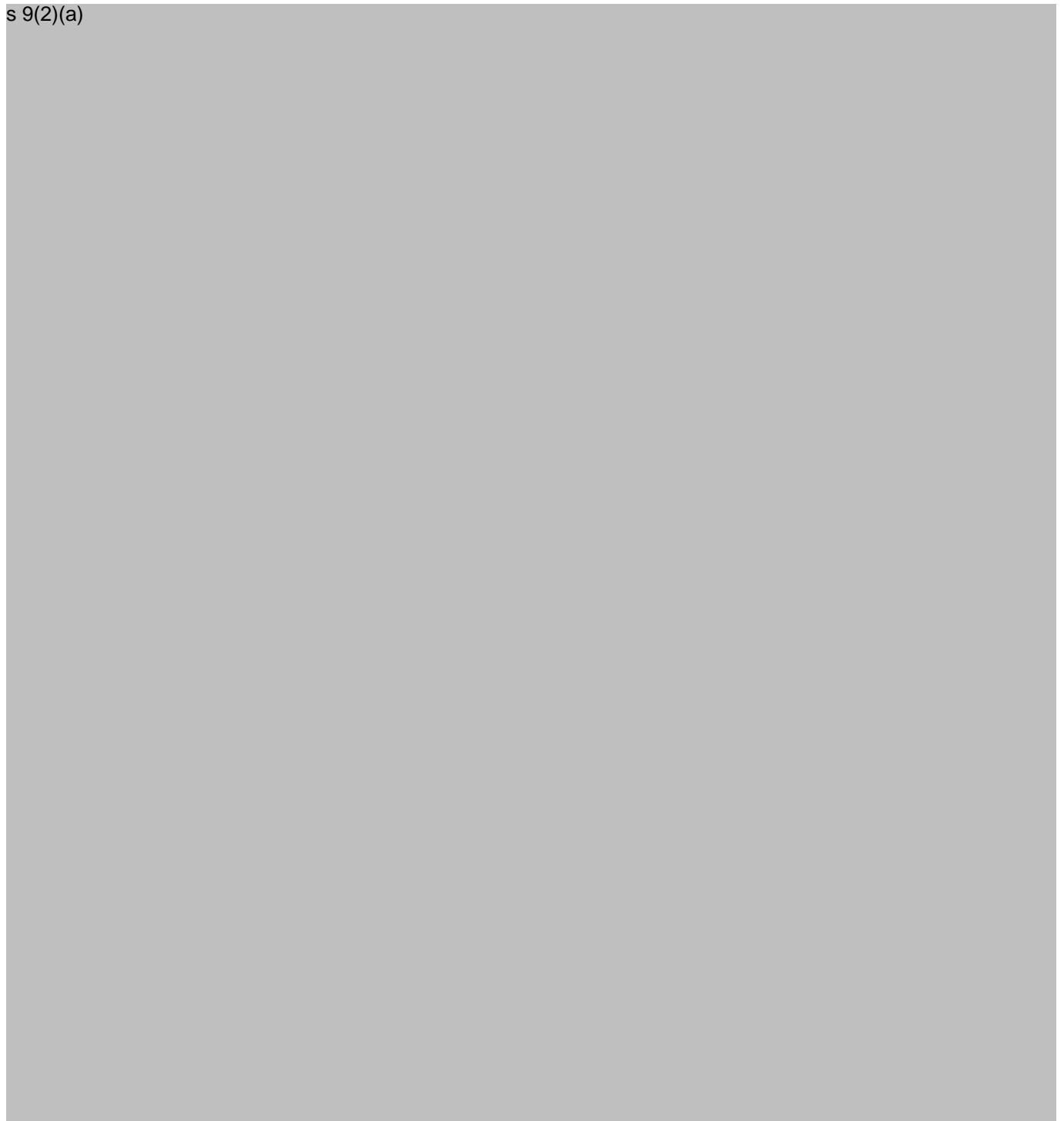
Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

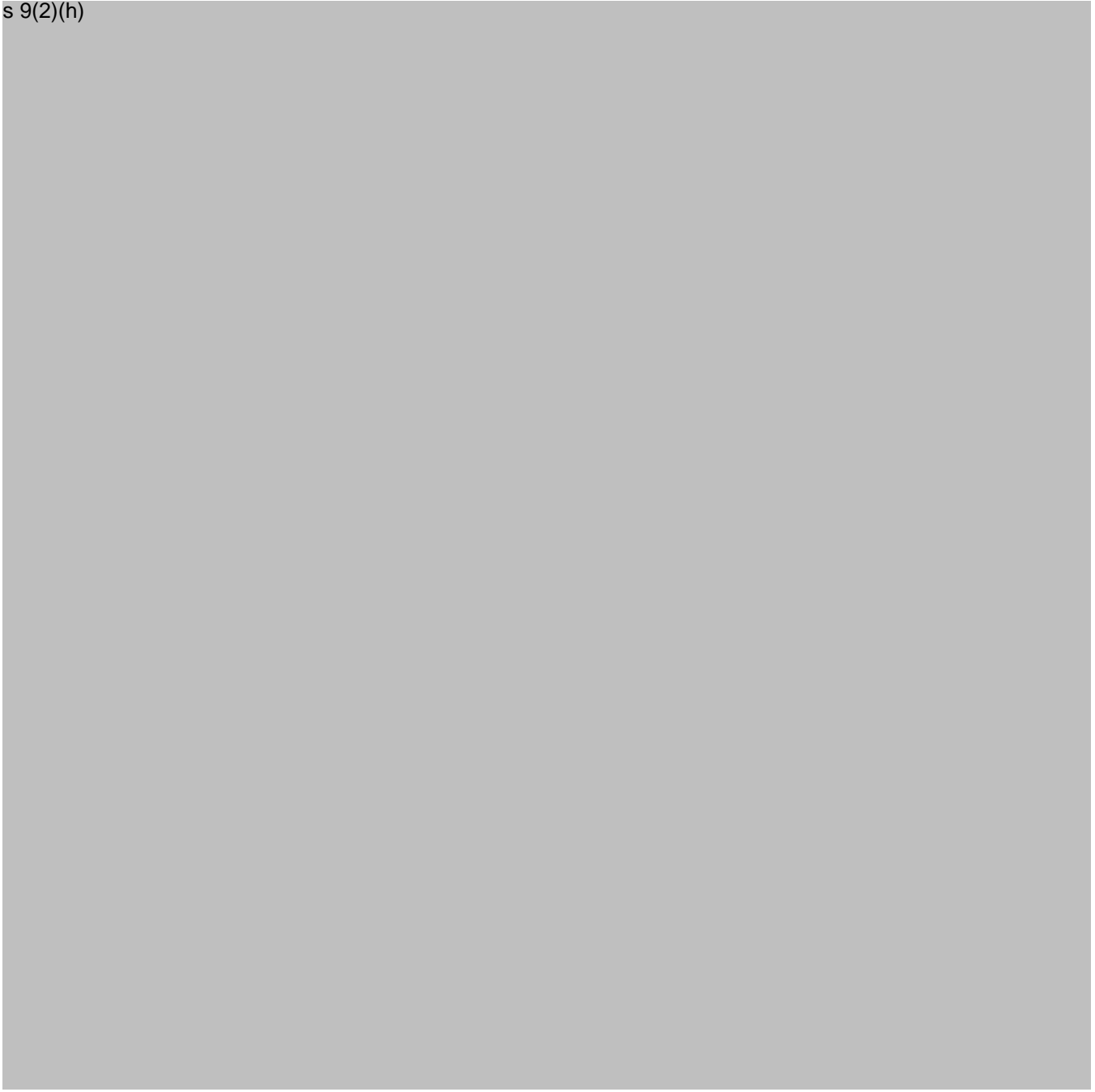
s 9(2)(a)



From: [Joanne Petrie](#)
To: [Karen Whitiskie](#); [Vanessa Johnson](#); [Dawn Swan](#)
Subject: s 9(2)(h)
Date: Thursday, 28 April 2022 9:30:47 am

Morena – if we are proposing to advise before the end of the week, I will schedule a meeting for later today/tomorrow with you all as well as Josh, Conrad, Gay – anyone else?


s 9(2)(h)



From: [Joanne Petrie](#)
To: [Vanessa Johnson](#); [Dawn Swan](#); [Karen Whitiskie](#)
Subject: s 9(2)(h)
Date: Thursday, 28 April 2022 8:56:15 am
Attachments: [image001.png](#)


We will also need to consider the Minister's Office as well. Perhaps once we have a timeline for when those people will be notified we can meet prior to line everything up and also ensure that Naomi/Cath are happy with the proposed response etc

s 9(2)(h)



From: Dawn Swan s 9(2)(a)
Sent: Thursday, 28 April 2022 8:17 AM
To: Karen Whitiskie s 9(2)(a); Vanessa Johnson
s 9(2)(a)
Cc: Joanne Petrie s 9(2)(a)
Subject: s 9(2)(h)

s 9(2)(h)



I would like to notify the Privacy Commissioner today instead of waiting until the end of the week. They expect breaches to be notified within 72 hours of an agency becoming aware although I think we have reasonable justification for why we did not do this – it came to light on the Thursday before Easter, we had public holiday long weekends and we were waiting to see if the USB could be located in that time. I don't see any further reason to delay informing them if we agree that notification should now occur.

There's an online notification form to inform the Privacy Commissioner which I can do today and we can then work on notifying those affected. I have a template letter that contains the necessary information that needs to be in a notification which I can also start drafting and send around for further detail to be included. What do we think of that approach?

Dawn Swan

Privacy Officer | Enterprise Design & Integrity | Inland Revenue

Asteron Centre, 55 Featherston Street, Wellington

PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or s 9(2)(a)


From: [Joanne Petrie](#)
To: [Dawn Swan](#); [Vanessa Johnson](#); [Karen Whitiskie](#)
Subject: s 9(2)(h)
Date: Thursday, 28 April 2022 8:37:36 am
Attachments: [image001.png](#)

Perhaps not at that forum Dawn – I would do it direct to Gay

From: Dawn Swan
Sent: Thursday, 28 April 2022 8:24 am
To: Vanessa Johnson ; Karen Whitiskie
Cc: Joanne Petrie
Subject: s 9(2)(h)

Yes, I have the Issues Management meeting at 8.30 that Gay runs so can give her a heads up then that we will be notifying, and we can get her input into the notification letters.

Not in scope, Duplicate





From: s 9(2)(a)
Sent: Friday, 29 April 2022 8:43 am
To: Karen Whitiskie
Cc: s 9(2)(a)
Subject: RE: Query
Attachments: CD recordings.pdf

Hi Karen,

The 10 recordings were for:

s 18(c)(i)

In terms of where people fit in s 18(c)(i)

The other 7 individuals s 18(c)(i)

I will need to compile a list of the call recordings list in the office.

Regards,

s 9(2)(a)

From: Karen Whitiskie
Sent: Friday, 29 April 2022 7:59 am
To: Andrew Instone
Cc: s 9(2)(a)
Subject: RE: Query

Hi s 9(2)(a)

Thanks for this and the other information.

s 9(2)(h)

Thanks

Karen

From: s 9(2)(a)
Sent: Thursday, 28 April 2022 5:37 PM
To: Karen Whitiskie s 9(2)(a)
Subject: RE: Query

Hi Karen,

Attached are the transcripts for the recordings,

There are 11 transcripts here, but there were only 10 recordings on the USB. This is due to one of the recordings not being located when we were looking to burn the CD's.

Regards,

From: Karen Whitiskie s 9(2)(a)
Sent: Thursday, 28 April 2022 3:20 pm
To: s 9(2)(a)
Cc: s 9(2)(a) s 9(2)(a)
Subject: RE: Query

Hi s 9(2)(a)

Can you send me the transcripts?

Thanks

Karen

From: s 9(2)(a)
Sent: Wednesday, 20 April 2022 2:44 PM
To: Karen Whitiskie s 9(2)(a)
Cc: s 9(2)(a) s 9(2)(a)
Subject: RE: Query

Hi Karen, s 9(2)(a)

We do have transcripts,

s 9(2)(h)

Regards,

From: s 9(2)(a)
Sent: Friday, 29 April 2022 12:02 pm
To: Karen Whitiskie
Subject: RE: Query

Yes one had two recordings so only 9 people affected in total

From: Karen Whitiskie
Sent: Friday, 29 April 2022 9:44 am
To: s 9(2)(a)
Cc: s 9(2)(a)
Subject: RE: Query

Hi Andrew

Who was the 10th person or was there one person twice on the recordings?

Thanks

Karen

From: s 9(2)(a)
Sent: Friday, 29 April 2022 9:15 AM
To: Karen Whitiskie s 9(2)(a)
Cc: s 9(2)(a) s 9(2)(a)
Subject: RE: Query

Hi Karen,

s 9(2)(h)

Regards,

s 9(2)(a)

From: Karen Whitiskie s 9(2)(a)
Sent: Friday, 29 April 2022 7:59 am
To: s 9(2)(a)

Cc: s 9(2)(a) s 9(2)(a)

Subject: RE: Query

Hi s 9(2)(a)

Thanks for this and the other information.

s 9(2)(h)

Thanks

Karen

From: s 9(2)(a)

Sent: Thursday, 28 April 2022 5:37 PM

To: Karen Whitiskie s 9(2)(a)

Subject: RE: Query

Hi Karen,

Attached are the transcripts for the recordings,

There are 11 transcripts here, but there were only 10 recordings on the USB. This is due to one of the recordings not being located when we were looking to burn the CD's.

Regards,

From: Karen Whitiskie s 9(2)(a)

Sent: Thursday, 28 April 2022 3:20 pm

To: s 9(2)(a)

Cc: s 9(2)(a) s 9(2)(a)

Subject: RE: Query

Hi s 9(2)(a)

Can you send me the transcripts?

Thanks

Karen

From: s 9(2)(a)

Sent: Wednesday, 20 April 2022 2:44 PM

To: Karen Whitiskie s 9(2)(a)

Cc: s 9(2)(a) s 9(2)(a)

Subject: RE: Query

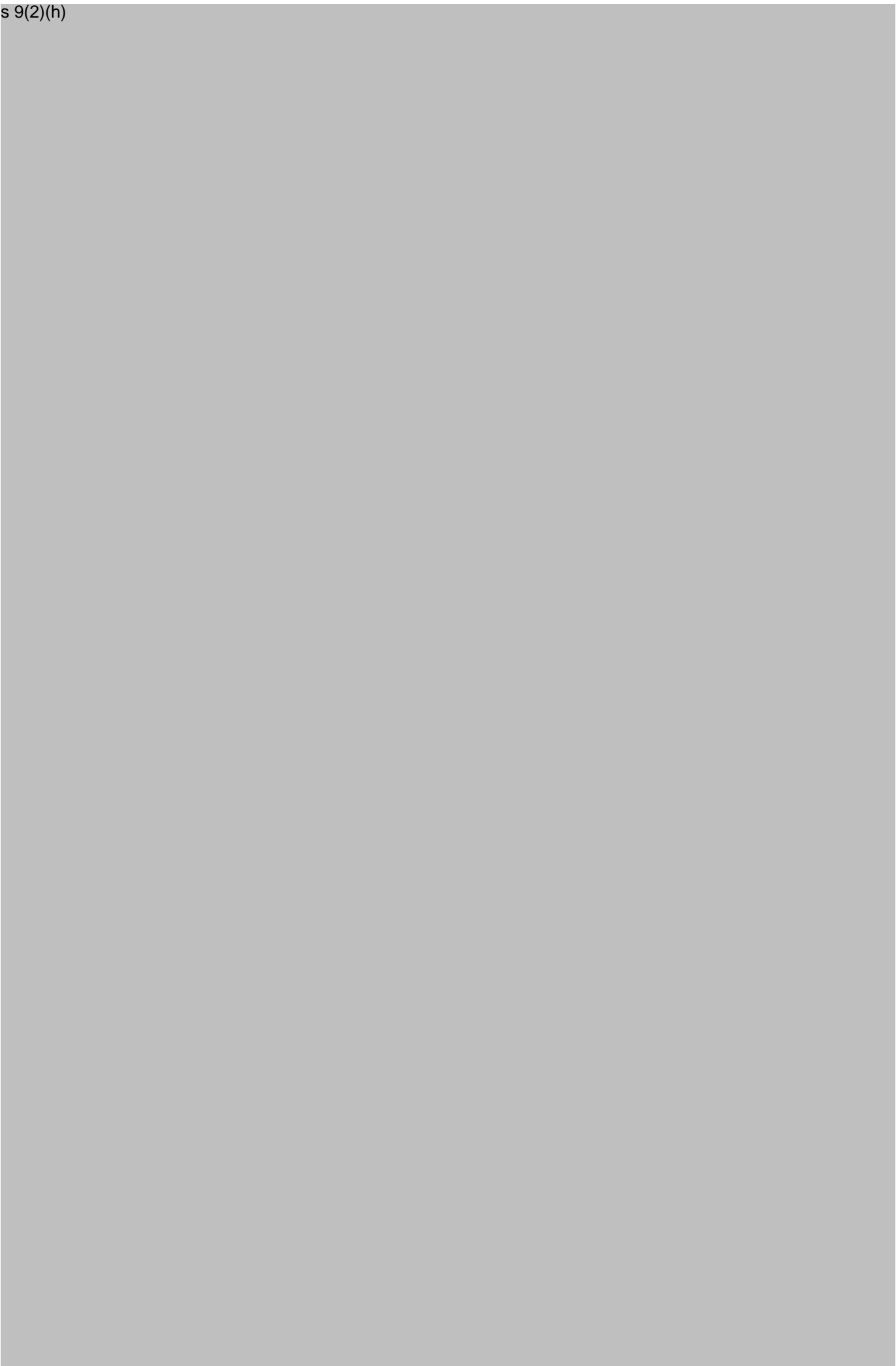
Hi Karen, s 9(2)(a)

We do have transcripts,

s 9(2)(h)

Regards,

Not in scope, Duplicate









From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: FW: s 18(c)(i)
Date: Monday, 2 May 2022 8:07:16 am
Attachments: [image001.jpg](#)
[image002.jpg](#)
[image003.jpg](#)
[image004.jpg](#)
s 9(2)(a)

[IN CONFIDENCE]

From: s 9(2)(a)
Sent: Sunday, 1 May 2022 11:09 am
To: s 9(2)(a)
Subject: s 18(c)(i)

External Email CAUTION: Please take **CARE** when opening any links or attachments.

From s 18(c)(i)
s 9(2)(a)
Department of Corrections Ara Poutama Aotearoa
s 18(c)(i)
s 9(2)(a)

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
|  |  |  |  |

The information in this message is the property of the New Zealand Department of Corrections. It is intended only for the person or entity to which it is addressed and may contain privileged or in confidence material. Any review, storage, copying, editing, summarising, transmission, retransmission, dissemination or other use of, by any means, in whole or part, or taking any action in reliance upon, this information by persons or entities other than intended recipient are prohibited. If you received this in error, please contact the sender and delete the material from all computers.

From: Dawn Swan
To: Vanessa Johnson; Karen Whitiskie; Joanne Petrie; Cath Atkins; Jay Harris
Subject: FW: Privacy Breach Notification
Date: Monday, 2 May 2022 4:20:51 pm
Attachments: image001.jpg
image002.png
image003.jpg
image004.png

FYI – a response from the Privacy Commissioner to our notification. They have closed the file.

@Jay Harris if we have a policy around use of USBs we should ensure that it states passwords should be transmitted via a different channel.

Dawn Swan

Privacy Officer | Enterprise Design & Integrity | Inland Revenue

Asteron Centre, 55 Featherston Street, Wellington

PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or s 9(2)(a)

From: s 9(2)(a)

Sent: Monday, 2 May 2022 3:16 PM

To: Dawn Swan

Subject: Privacy Breach Notification

External Email CAUTION: Please take **CARE** when opening any links or attachments.

Dawn,

Thank you for notifying us of this privacy breach incident. I have recorded it as PBN/1068.

I am sure you (and your IT security people) are as disappointed as I am that the password was on a post-it note. If your policies do not already cover this area, I would suggest that they be amended to require that passwords be transmitted by a different channel from the files.

I have closed our file, but please provide an update if any further developments arise.

Regards,

Neil.

s 9(2)(a)

Senior Compliance Adviser

Office of the Privacy Commissioner Te Mana Mātāpono Matatapu

PO Box 10094, The Terrace, Wellington 6143

Level 11, 215 Lambton Quay, Wellington, New Zealand

s 9(2)(a)

E compliance and enforcement team inbox: compliance@privacy.org.nz

privacy.org.nz

Privacy is about protecting personal information, yours and others.

Training modules are online and free at: <https://privacy.org.nz/tools/online-privacy-training-free/>

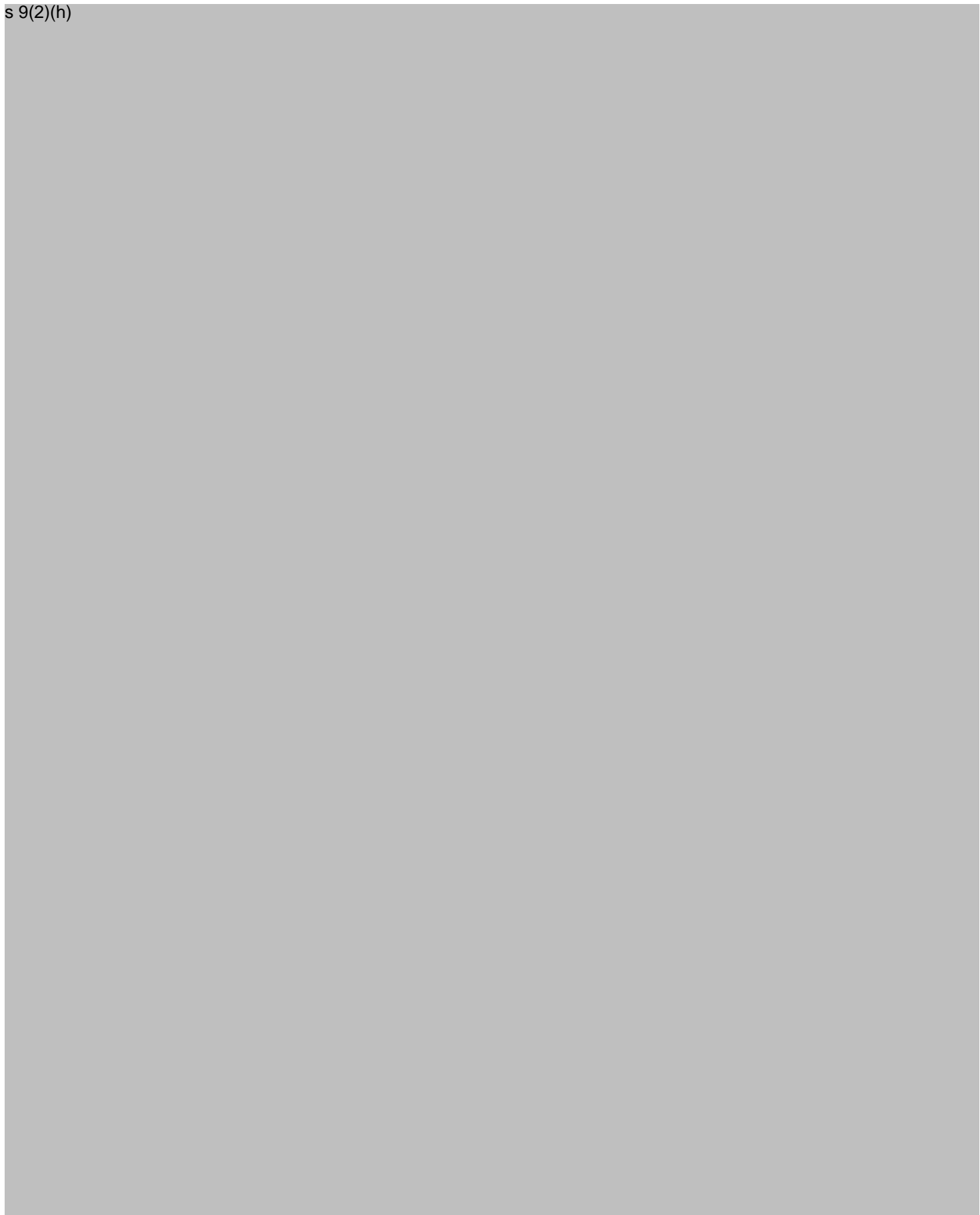
Questions about Privacy? Try: [AskUs](#)

To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.  

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments.

Please treat the contents of this message as private and confidential. Thank you.





From: [Joanne Petrie](#)
To: [Karen Whitiskie](#); [Naomi Ferguson](#); [Cath Atkins](#); [Vanessa Johnson](#); [Josh Green](#); [Kirsty Gemmill](#)
Cc: [Gay Cavill](#); [Rowan McArthur](#); [Jay Harris](#); [Mary Craig](#)
Subject: PSC Conversation
Date: Friday, 6 May 2022 1:52:50 pm

Kia ora

I have spoken with Martin Kessick at PSC and covered off the following questions he had:

- Confirmed the Minister/office has been advised as appropriate.
- IR has a process/protocols in place for transporting this type of device
- This was an employee not a contractor or courier delivering the stick
- We have processes/protocols/policies in place for this to not happen again
- Confirmed we are not able to track digitally if anyone has accessed the stick
- The device was not lost while travelling on public transport/a plane
- Media is in place to manage this

He will come back with any further queries if Peter/Helene need any further clarification and see how this runs over the weekend.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)



Inland Revenue

Privacy Breach Process Manual

Senior Responsible Owner: Paul Le Sueur

Project Sponsor: James Grayson

Prepared by:
Date:

Catherine Lee
16 April 2021 v3.0

About this Document

This document outlines the Privacy Breach process and provides an end to end view of the handling of a privacy breach. **Note:** This document is a living document and will be updated as and when operational processes and information changes.

Document Control

| | |
|---------------------------|----------------------------------|
| File Name and Path | Privacy Breach Operating Manual |
| | C&O Events Management Teams Page |
| Contact Person | Catherine Lee |
| Status | Final |
| Template Version | 4 |

Document Review History

| No | Date | Change Description | Contact |
|----|------------|--|---------------|
| 1 | 11/11/2020 | Initial Draft | Catherine Lee |
| | 27/11/2010 | Sent for review | Catherine Lee |
| 2 | 14/04/2021 | Updated with new ServiceNow details and feedback from Dawn | Catherine Lee |
| 3 | 16/04/2021 | Final | Catherine Lee |
| 4 | 10/03/2022 | Update with changes regarding archived documents at TIMG | Catherine Lee |
| | | | |
| | | | |
| | | | |
| | | | |

Document Signoff

| Formal Review Area | Name | Signature | Date |
|---|---|-----------|------|
| Responsible person | Paul Le Sueur | | |
| The following people have supported the development of this document: | Dawn Swan (IR Privacy Officer) Jacqui Dannefaerd Tina Banks | | |

| | |
|--|-----------|
| 1 Document Overview | 4 |
| Definitions/Acronyms..... | 4 |
| Key Contacts | 4 |
| Service Desk Assignment Queues | 4 |
| 2 Background | 5 |
| 2.1 What is “privacy”?..... | 5 |
| 2.2 The Privacy Act 2020..... | 6 |
| 2.3 Notifiable privacy breaches..... | 7 |
| 3 Responding to and managing a privacy breach..... | 9 |
| Step 1: Breach containment and initial assessment | 9 |
| Step 2: Evaluate the risks associated with the breach | 9 |
| Step 3: Notification | 9 |
| Step 4: Prevent future breaches | 10 |
| 3.1 Notifiable privacy breach process | 11 |
| 3.2 Priority definitions for privacy breach | 13 |
| 4 Privacy Breach Operating Process | 14 |
| 5 Business process steps | 15 |
| 6 Reporting requirements and lessons learned..... | 18 |
| 6.1 Monthly report to the Privacy Officer..... | 18 |
| 6.2 Lessons learned..... | 20 |
| 6.3 Collaboration meeting | 20 |
| 7 Appendix 1 – Privacy Breach Notification Form Example | 21 |
| 8 Appendix 2 – Delete documents in TIMG archive..... | 22 |

1 Document Overview

Note: This document is a living document and will be updated as and when operational processes, procedures and information changes

Definitions/Acronyms

| Terms/Acronyms | Definition |
|---|--|
| ServiceNow (SNow) | IR system to support ITIL and related functions. Used by many including IR Service Provider/IR Support Teams and the IR Service Desk |
| SLA | Service Level Agreement: Performance agreements between the business incident team and IR |
| The Information Management Group (TIMG) | Storage facility for IR's archived documents. Replacement for EDSR. |

Key Contacts

The following table contains the key contacts for roles involved in Privacy Breach management in IR.

This table should be reviewed and updated on a regular basis to ensure currency.

| Contact | Contact details | Current contact person |
|---|--|--------------------------------|
| Deputy Commissioner Enterprise Design and Integrity | s 9(2)(a) [Redacted] [Redacted] [Redacted] | Mary Craig |
| Privacy Officer | s 9(2)(a) [Redacted] [Redacted] [Redacted] | Dawn Swan |
| Capability & Outcomes - Business Incident Team | s 18(c)(i) [Redacted] | Paul Le Sueur Catherine Lee |

Service Desk Assignment Queues

| Service Provider | ServiceNow Assignment Queue | Purpose |
|------------------------|-----------------------------|--------------------|
| Business Incident Team | ASGN-BusinessServiceMgmt | Business incidents |
| Business Incident Team | FUNC-Privacy Breaches | Privacy breaches |

2 Background

2.1 What is “privacy”?

Privacy can mean different things to different people, but the Privacy Act is focused on **personal information** and how it’s managed.

Personal information is defined in the Privacy Act as information about an identifiable person, so the information must tell the reader something about a specific person. If no one is identified by the information, then it is not personal information.

This manual provides guidance when responding to privacy incidents that involve Inland Revenue’s (IR) customers or people.

A **privacy incident** happens when personal information is put at risk and a **privacy breach** is when there is unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information. Incidents can be accidental or deliberate and IR records both potential and actual breaches.

A privacy incident (or potential privacy breach) occurs where the information disclosed does not personally identify a customer but has the potential to do so if the information is not corrected.

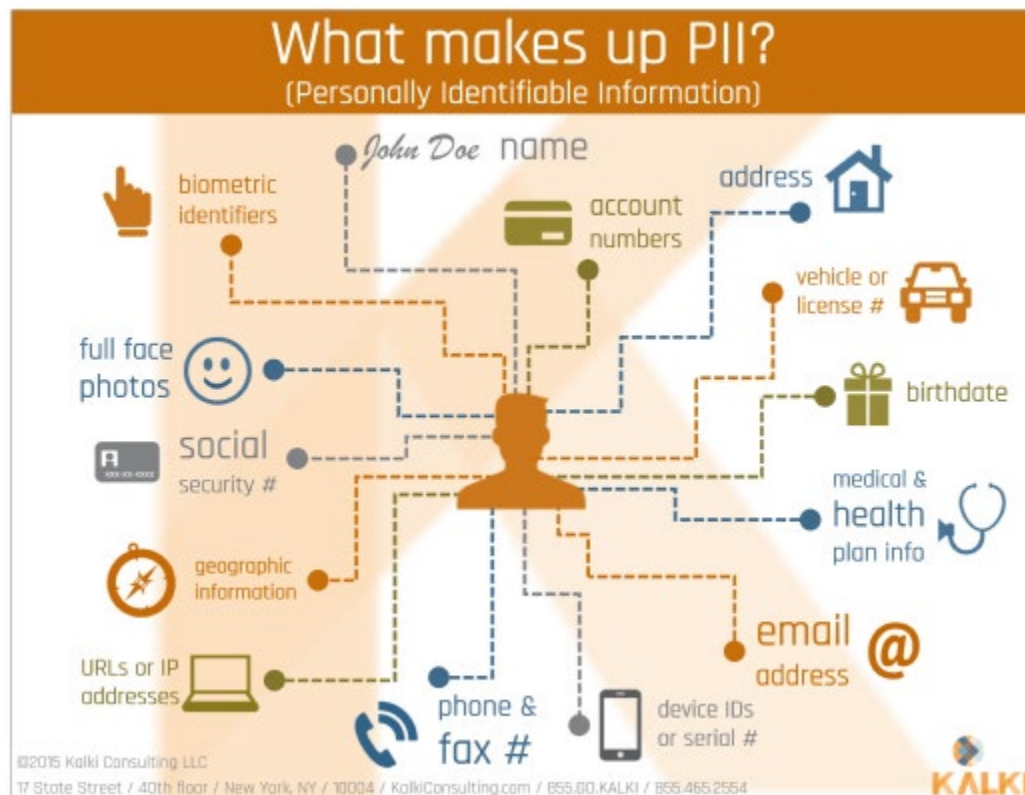
In these situations, we will classify as a potential breach and undertake some of the same corrective actions as that of a privacy breach.

Examples of a potential privacy breach might be:

- A letter being sent to a customer that contains information relating to another customer, but where the information disclosed is only the first name of another customer.
- A note being updated to the incorrect customer account, but no information has been disclosed.
- An email response being sent to the incorrect customer but is contained before any disclosure made.

Information about organisations (i.e. companies or trusts) is not personal information so will not usually amount to a privacy breach. However, putting company information at risk may be a breach of the confidentiality provisions in the Tax Administration Act.

All Inland Revenue employees have a responsibility to protect the integrity of the tax system. The public expect us to keep their information secure. Responding quickly and effectively to a privacy incident is imperative in order to contain a breach, safeguard our customers’ privacy and maintain the public’s and Minister’s trust and confidence in IR.



Inland Revenue holds and uses a lot of personal information so it must keep that information safe and only use it for specific purposes.

2.2 The Privacy Act 2020

The Privacy Act governs how individuals, organisations and businesses collect, use, disclose, store and give access to personal information. Personal information is defined as information about an identifiable, living person. If information does not identify anyone, the Privacy Act will not apply.

The Privacy Act applies to 'agencies'.

Almost every business, organisation, and individual that handles personal information is considered an agency under the Privacy Act – whether they are a government department, private company, religious group, school, or even an individual person in some cases.

At the heart of the Privacy Act are 13 privacy principles that state how agencies must treat personal information. These principles reflect internationally accepted standards for good personal information handling:

1. Only collect necessary personal information for a lawful purpose
2. Get information direct from the person concerned unless an exception applies

3. Tell people what you're going to do with their information
4. Don't collect information by means that are unfair or intrusive
5. Once you hold personal information, keep it secure
6. People are allowed to request, and have access to, their own information
7. People can ask for their information to be corrected
8. Information should be accurate before it is used
9. Don't keep information for longer than is necessary
10. You can't use personal information collected for one purpose for another unless an exception applies
11. You shouldn't disclose personal information unless an exception applies
12. When disclosing personal information overseas the country the information will go to must have comparable privacy protections to New Zealand.
13. Don't assign unique identifiers, or require someone to disclose one, unless it's lawful.

More information is available on Haukainga at [s 18\(c\)\(i\)](#)

2.3 Notifiable privacy breaches

Under sections 114 and 115 of the Privacy Act 2020 all agencies in New Zealand have to report notifiable privacy breaches to the Privacy Commissioner and affected individuals.

Under section 112 of the Privacy Act, a **privacy breach** in relation to personal information held by an agency means:

- i. unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or
- ii. an action that prevents the agency from accessing the information on either a temporary or permanent basis; and

(b) was caused by a person inside or outside the agency; or is attributable in whole or in part to any action by the agency; or is ongoing.

The factors that must be considered by an agency when assessing whether a privacy breach is likely to cause serious harm (section 113 of the Act) include:

- any action taken by the agency to reduce the risk of harm following the breach
- the sensitivity of the information (the more sensitive, the higher the risk of harm. A combination of personal information is usually more sensitive than a single piece of personal information).

- the nature of the harm that may be caused to affected individuals (is there a risk of identity theft, fraud or physical harm, or a risk of humiliation, loss of dignity, damage to the individual's reputation or relationships?)
- the person or body that has obtained or may obtain personal information as a result of the breach (if known). Information in the hands of people with unknown or malicious intentions can be of greater risk.
- whether the information protected by a security measure, for example is it encrypted?
- size of the breach – how many people can access the information; how many are affected?
- whether the breach has been contained.

IR staff don't have to assess harm, but do have to report a privacy breach using the online form [privacy breach notification form](#).

The C&O - Business Incident Team and Privacy Officer will decide if it's a notifiable privacy breach.

The Privacy Commissioner has developed a tool, [NotifyUs](#), for organisations to use to assess if privacy breaches are notifiable and submit them.

This self-assessment tool does not ask for any information that identifies the user and no information entered into the tool is sent to the Privacy Commissioner unless you elect to submit a privacy breach notification. So the tool can be used as a guide to determine if a breach should be notified.

If it is decided that IR has a notifiable privacy breach it should be submitted to the Privacy Commissioner using this [NotifyUs](#).

A failure to notify the Privacy Commissioner of a notifiable privacy breach can result in a \$10,000 fine.

3 Responding to and managing a privacy breach

If you come across a privacy breach, you must complete the [privacy breach notification form](#).

IR's Privacy Officer is also available to assist you with any questions relating to privacy breaches and when to complete the notification form.

At IR, privacy breaches are logged into ServiceNow and are managed by the C&O Capability and Outcomes Events & Business Incident Team with input from the Privacy Officer when necessary. Four key steps should be considered when responding to a privacy breach.

Step 1: Breach containment and initial assessment

- Stop the practice/action.
- Recover the records (if possible).
- Revoke or change computer access (if necessary).
- Ensure evidence is preserved (particularly when information has been stolen).
- Complete the [privacy breach notification form](#).

Step 2: Evaluate the risks associated with the breach

- Consider and identify what personal information was involved.
- Establish the cause and extent of the breach.
- Consider who is affected by the breach.
- Identify whether harm could result from the breach.

Step 3: Notification

Decide whether to notify the affected people. If the breach **is not likely to cause serious harm** to the individual it is not mandatory to notify them, but notification is transparent and provides customers with the opportunity to take steps to protect their personal information if necessary, such as by changing passwords or being alert to possible scams resulting from the breach.

If the breach is a notifiable privacy breach, see below for details.

It's important that staff engage with individuals who have been affected by a data breach with sensitivity and compassion, in order not to cause them further harm.

Each incident needs to be considered on a case-by-case basis to determine whether notification is necessary. If we do decide to notify, then do it promptly.

However, sometimes notifying individuals can cause undue stress or harm. For example, a data breach that poses little-to-no risk of harm can cause unnecessary anxiety. Don't notify people unless you're sure of the people whose information has been compromised by the breach. More damage can be done if the wrong people are notified.

When deciding whether to notify consider:

- What is the risk of harm to people whose information has been breached?
- Is there a risk of identity theft or fraud?
- Is there a risk of physical harm?
- Is there a risk of humiliation or loss of dignity, damage to the individual's reputation or relationships?
- What is the person's ability to avoid or minimise possible harm?
- Who should be contacted? For example, the Privacy Commissioner's office, Minister's office, Police, other internal and external parties.

Breach notifications should contain:

- Information about the incident, including when it happened.
- A description of the personal information that has been disclosed.
- What IR is doing to control or reduce the harm.
- What steps people can take to protect themselves if necessary.
- Contact information for enquiries and complaints.
- Offers of assistance when necessary; for example, advice on changing passwords or a link to [Identity Security information](#).

Step 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, investigations are required to determine the cause of the breach and whether a prevention plan should be developed.

3.1 Notifiable privacy breach process

If IR has a breach that will cause harm, or is likely to do so, the Privacy Commissioner and affected individuals must be notified.

3.1.1 When notification must occur

Notification must happen as soon as practicable after becoming aware that a notifiable privacy breach has occurred.

- **Notifying affected individuals**
Individuals should be notified directly or through a public notice of the breach where it's not reasonably practicable to notify an affected individual or each member of a group of affected individuals. Public notice must be given in a form in which no affected individual is identified.
- **Notifying the Privacy Commissioner**
A notifiable privacy breach is submitted to the Privacy Commissioner using the tool [NotifyUs](#) on the Privacy Commissioner's website.

There are some exceptions to notifying.

An agency is not required to notify affected individuals if the agency believes that the notification or notice would be likely to—

- (a) prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or
- (b) prejudice the maintenance of the law by any public sector agency, including the prevention, investigation, and detection of offences, and the right to a fair trial; or
- (c) endanger the safety of any person; or
- (d) reveal a trade secret or
- (e) if the individual is under the age of 16 and the agency believes that the notification or notice would be contrary to that individual's interests.

An agency may also delay notifying an affected individuals (but not delay notifying the Privacy Commissioner) only if the agency believes a delay is necessary because notification or public notice may have risks for the security of personal information held by the agency and those risks outweigh the benefits of informing affected individuals.

3.1.2 Requirements for notification

A notification to the Privacy Commissioner must:

- a. describe the notifiable privacy breach, including—
 - i. the number of affected individuals (if known); and
 - ii. the identity of any person or body that the agency suspects may be in possession of personal information as a result of the privacy breach (if known); and

- b. explain the steps taken or intended to take in response to the privacy breach, including whether any affected individual has been or will be contacted; and
- c. if giving public notice of the breach, set out the reasons for doing so; and
- d. if the agency is relying on an exception, or is delaying notifying affected individuals or giving public notice, state reasons why; and
- e. name or give a general description of any other agencies that the agency has contacted about the privacy breach and the reasons for having done so; and
- f. give details of a contact person within the agency for inquiries.

A notification to an affected individual must:

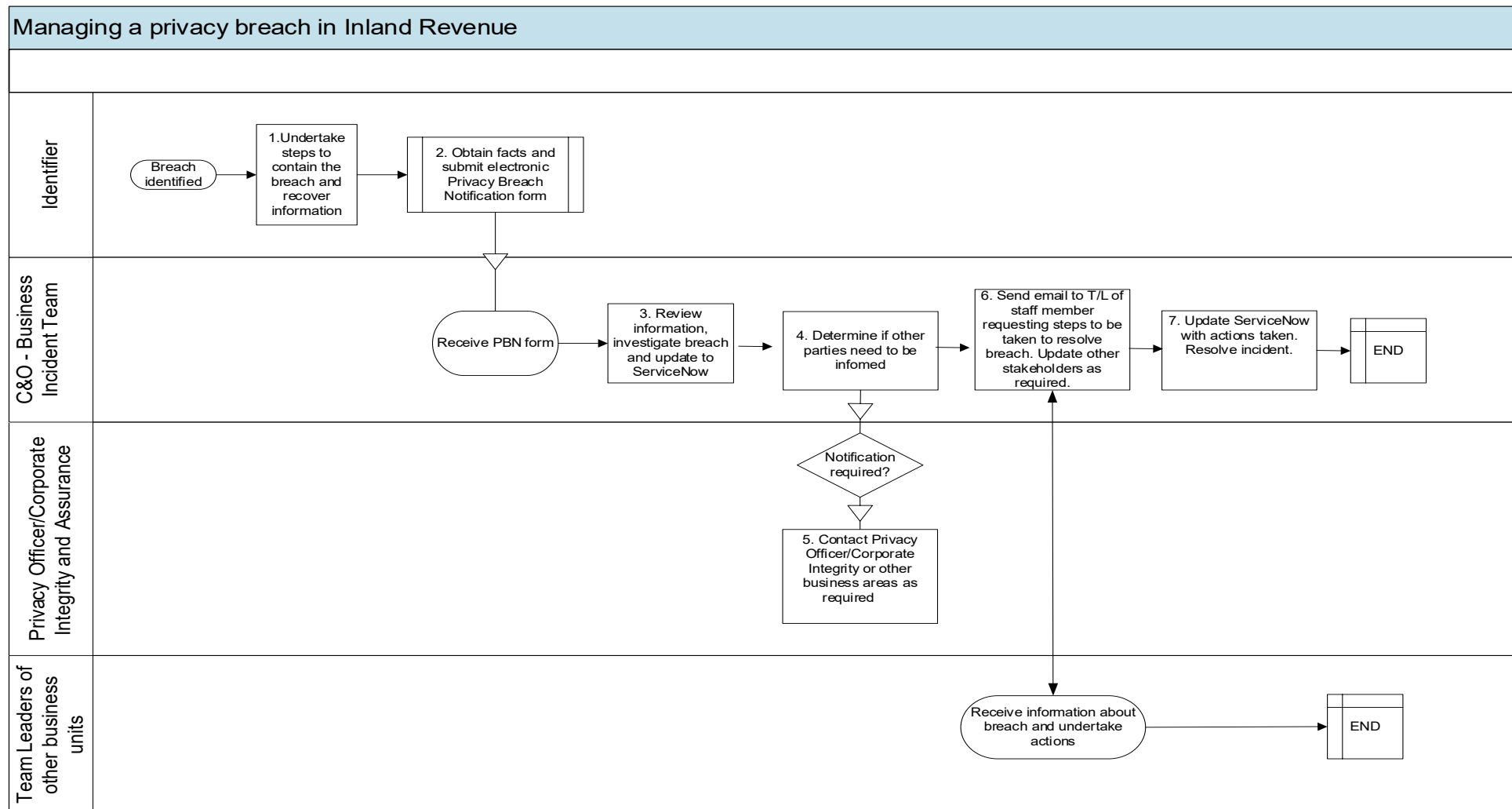
- a. describe the notifiable privacy breach (include exactly what information is involved and the date it occurred) and state whether the agency has or has not identified any person or body that the agency suspects may be in possession of the affected individual's personal information (but must not include any particulars that could identify that person or body); and
- b. explain the steps taken or intended to be taken by the agency in response to the privacy breach; and
- c. where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any); and
- d. confirm that the Privacy Commissioner has been notified; and
- e. state that the individual has the right to make a complaint to the Privacy Commissioner; and
- f. give details of a contact person within the agency for inquiries.

3.2 Priority definitions for privacy breach

When determining priority, consideration is given to: customer group and the numbers affected; customer expectations and compliance activity; consequences if not resolved urgently; the impacts to the business e.g. financial, rework, ability to deliver good service; risk posed to IR in terms of reputation and confidence; senior management and ministerial requirements.

| Term | Description |
|------------------------------|--|
| Priority 1 - Critical | <ul style="list-style-type: none"> • Privacy breach that threatens to hit the media • Significant impact to IR's reputation, compliance, privacy or security • Widespread impact to IR customers or key group of customers • Requires significant work effort to resolve • Has significant financial implications • A notifiable privacy breach <p>P1 incidents have a 7 day Service Level Agreement</p> |
| Priority 2 - High | <ul style="list-style-type: none"> • Moderate impact to IR's reputation, compliance, privacy or security • Moderate impact to IR customers or key group of customers • Moderate level of financial implications <p>P2 incidents have a 7 day Service Level Agreement</p> |
| Business Priority 3 - Medium | <ul style="list-style-type: none"> • Low impact to IR's reputation, compliance, privacy or security • Low impact to IR customers • Privacy breach is contained <p>P3 incidents have a 10 day Service Level Agreement</p> |

4 Privacy Breach Operating Process



5 Business process steps

Use this process to understand how a privacy/potential privacy breach incident is to be triaged.

| # | Process step name | Description | Responsible team |
|----|---|--|-------------------------------------|
| 1. | Undertake steps to contain the breach and recover information | Staff member: <ul style="list-style-type: none"> Identifies a privacy breach Takes steps to contain it. | Staff member |
| 2. | Obtain facts and submit Privacy Breach Notification form in ServiceNow | Staff member: <ul style="list-style-type: none"> Obtains facts Submits electronic privacy breach notification form. | Staff member |
| 3. | Review information, investigate breach, prioritise and update to ServiceNow | Business incident team: <ul style="list-style-type: none"> Review information in submission form to ensure enough detail received Investigate details of breach to determine that it is a privacy/potential breach <p>If a privacy/potential breach:</p> <ul style="list-style-type: none"> Prioritise breach in ServiceNow Manage as privacy/potential breach <p>If not a privacy/potential breach:</p> <ul style="list-style-type: none"> Manage as business incident | C&O-Events & Business incident team |
| 4. | Determine if other parties need to be informed | After investigation of details may need to inform other parties. | C&O-Events & Business incident team |

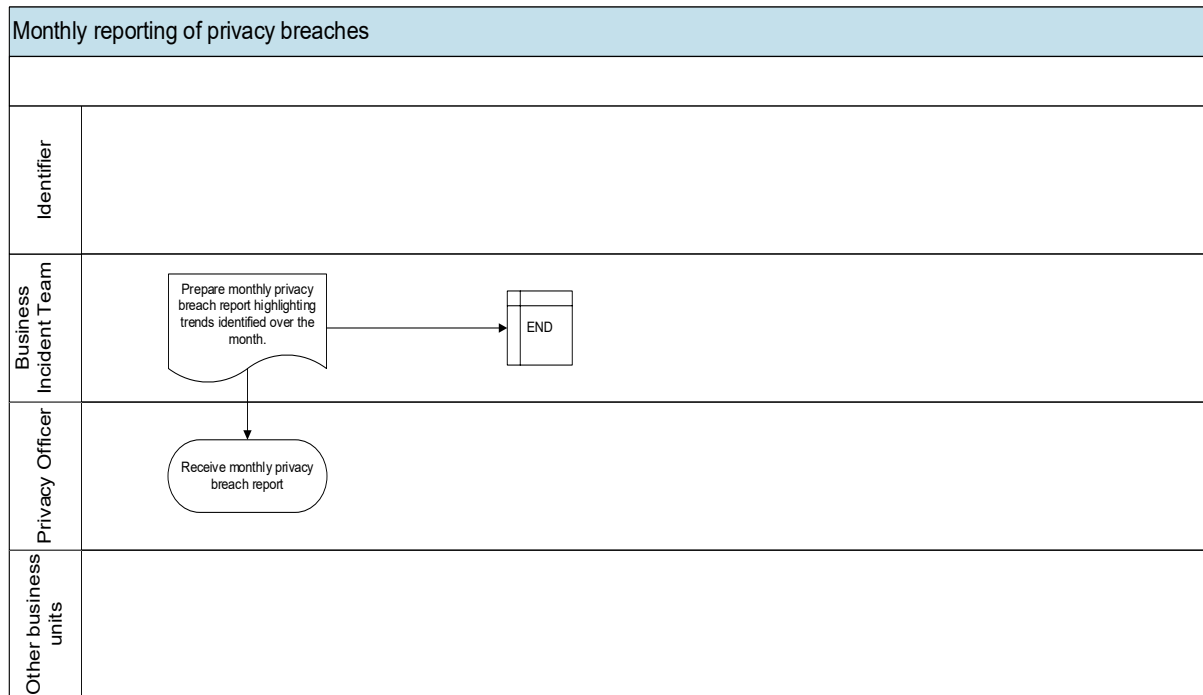
| # | Process step name | Description | Responsible team |
|----|--|--|-------------------------------------|
| 5. | Contact Privacy Officer/Corporate Integrity & Assurance or other business areas as required | <p>If clarification required:</p> <ul style="list-style-type: none"> • Contact Privacy Officer for assistance <p>If staff Code of Conduct issue:</p> <ul style="list-style-type: none"> • Hand off details to Corporate Integrity & Assurance s 18(c)(i) | C&O-Events & Business incident team |
| 6. | Send email to T/L of staff member requesting steps to be taken to resolve breach. Update other stakeholders as required. | <p>Business incident team:</p> <ul style="list-style-type: none"> • Send email to the Team Leader of the staff member that caused the breach advising of the details of the breach. • Request that the Team Leader undertake actions required to resolve the breach which may include: <ul style="list-style-type: none"> - Contacting the customers impacted to advise of breach and to apologise. - Update and correct customer accounts. - Letter or email of apology - Discussion with staff/training required to prevent a reoccurrence - Request a response back to the Incident Team on progress and resolution. • If required arrange for an appropriate team to undertake data purification. • If required arrange for incorrectly issued letter to be deleted in TIMG or invalidated in START. • If required organise communications to staff through Snapshot or service alerts. | C&O-Events & Business incident team |

| # | Process step name | Description | Responsible team |
|----|---|---|-------------------------------------|
| | | <ul style="list-style-type: none"> If privacy breach is a P1 may need to send communication to a wider audience. | |
| 7. | Update ServiceNow with actions taken. Resolve incident. | <p>Business incident team:</p> <ul style="list-style-type: none"> Update ServiceNow with details of the steps taken to resolve. Check to see if other actions are required to be completed Check customer account to ensure corrections made and account updated Issue communications to staff if required If all steps completed the incident is updated to 'Resolved' in ServiceNow | C&O-Events & Business incident team |

Note:

| If... | then... |
|--|---|
| a privacy breach is classified as a P1 | <p>A business decision may be made for the privacy breach to be managed by a senior IR manager or the Major Incident Team. The business incident team will support as necessary.</p> <p>If the P1 privacy breach is managed by the business incident team the normal operating processes are followed. There will be additional communications notified to other key stakeholders. This may include the following:</p> <ul style="list-style-type: none"> Media Team Commissioner's office Privacy Officer/Corporate Integrity & Assurance C&O leadership team CCS-I leadership team CCS-B leadership team IR Major Incident Management team |

6 Reporting requirements and lessons learned

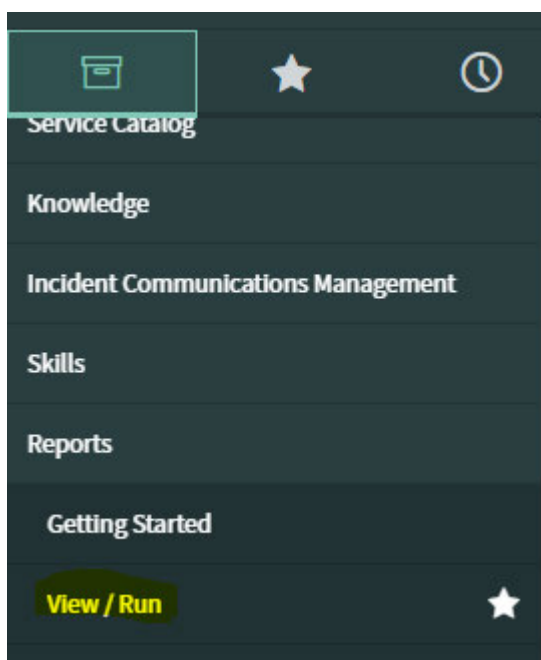


6.1 Monthly report to the Privacy Officer

At the beginning of each month a report is run out of ServiceNow extracting details for the previous month relating to notified privacy breaches and potential breaches.

This report is expected to be completed and sent to the Privacy officer no later than 7 working days after the end of the month.

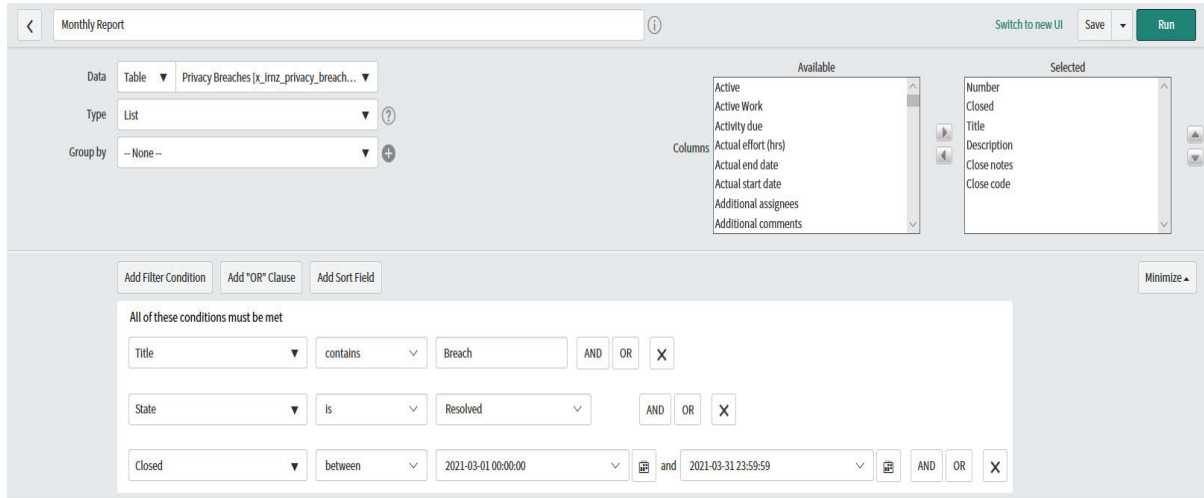
Report request in ServiceNow:



Select "View/Run"

Select "Monthly Report"

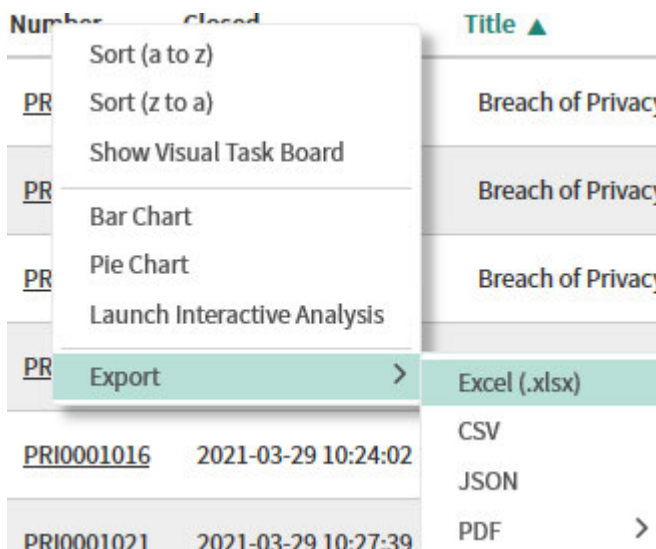
Update the "Closed" condition - enter the start and end date of the monthly period



Click "Save" then click "Run" to create the report.

The details will display as a list.

Right click on the "Number" field and Export to an Excel spreadsheet.



| Number | Closed | Title |
|------------|---------------------|-------------------|
| PR | | Breach of Privacy |
| PR | | Breach of Privacy |
| PR | | Breach of Privacy |
| PR | | Breach of Privacy |
| PRI0001016 | 2021-03-29 10:24:02 | |
| PRI0001021 | 2021-03-29 10:27:39 | |

The report includes the following details:

- **Number** – Privacy breach number assigned in ServiceNow
- **Closed** – Date privacy breach resolved
- **Title** – Heading details of breach
- **Description** – Brief summary of the details of the breach
- **Close notes** – Actions taken to resolve breach

The following headings are then added to the spreadsheet, the details of which are determined from the information in the privacy breach notification form. These are required by the Privacy Officer:

- **Subcategory** – whether it was a privacy breach or a potential breach
- **Customers impacted** - number of customers impacted by the breach
- **Media** – the method by which the breach occurred.

Example of report to Privacy Officer:

| Number | Resolved | Short description | Description | Close notes | Subcategory | Customers Impacted | Media |
|------------|-----------|--|---|------------------------------------|------------------|--------------------|--------|
| INC0247107 | 6/10/2020 | Potential Breach_CS_CS005 letter issued to receiving carer in error. s 18(c)(i) | Letter named the employer of the other parent, the amount owing, and the deduction amount to be made, but did not mention the other parent's name at all. | Email sent to T/L. Letter deleted. | Potential Breach | | Letter |
| INC0247269 | 6/10/2020 | Breach of Privacy_CS_Disclosure of information s 18(c)(i) | Officer advised liable parent that the receiving carer was on a sole parent benefit | T/L advised | Privacy breach | 1 | Phone |
| | | | | | | 1 | |

6.2 Lessons learned

As part of the monthly reporting process to the Privacy Officer, include a summary of the lessons learned and/or common themes identified from the report.

This will enable the Privacy Officer or Events Team to:

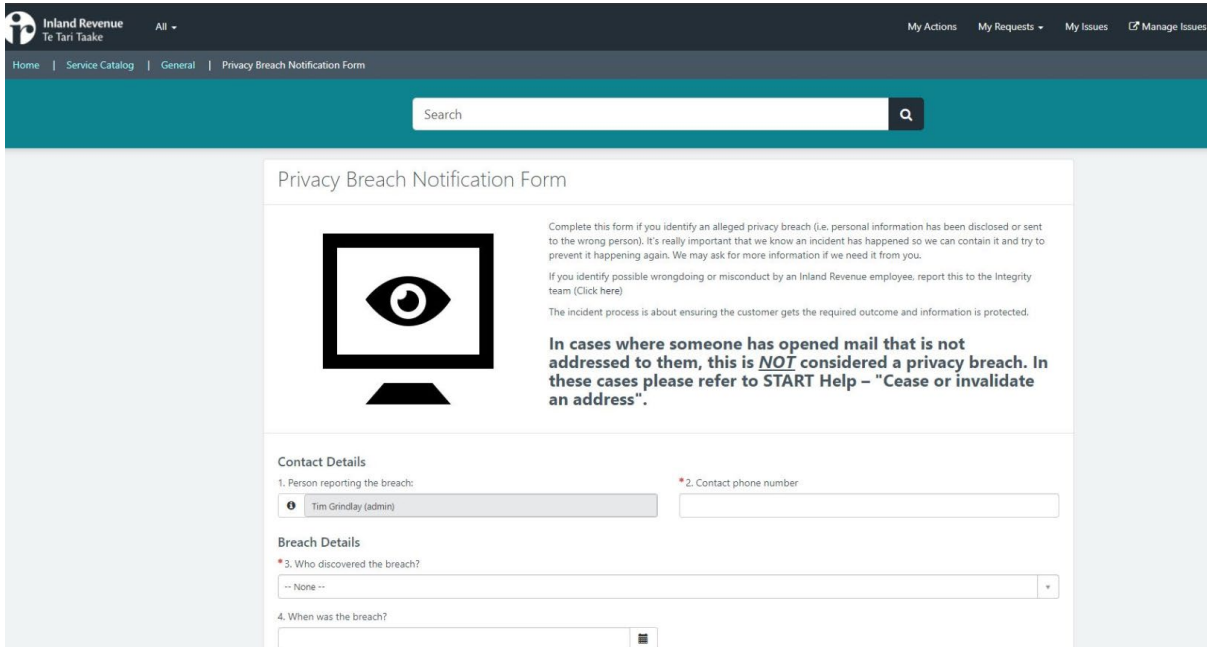
- Identify and update possible gaps in the START Help information for staff
- Provide feedback to the business around possible process improvements
- Identify opportunities for staff training
- Issue general staff reminders through Snapshot, Featured News or other channels

6.3 Collaboration meeting

As part of the recent privacy breach audit review, a monthly meeting was established between IKM and privacy SME's (Capability & Outcomes - Events Team and Privacy Officer) to discuss arising privacy risks that IKM identify through their work, and to determine areas of collaboration where IKM campaigns can be leveraged for communicating important lessons.

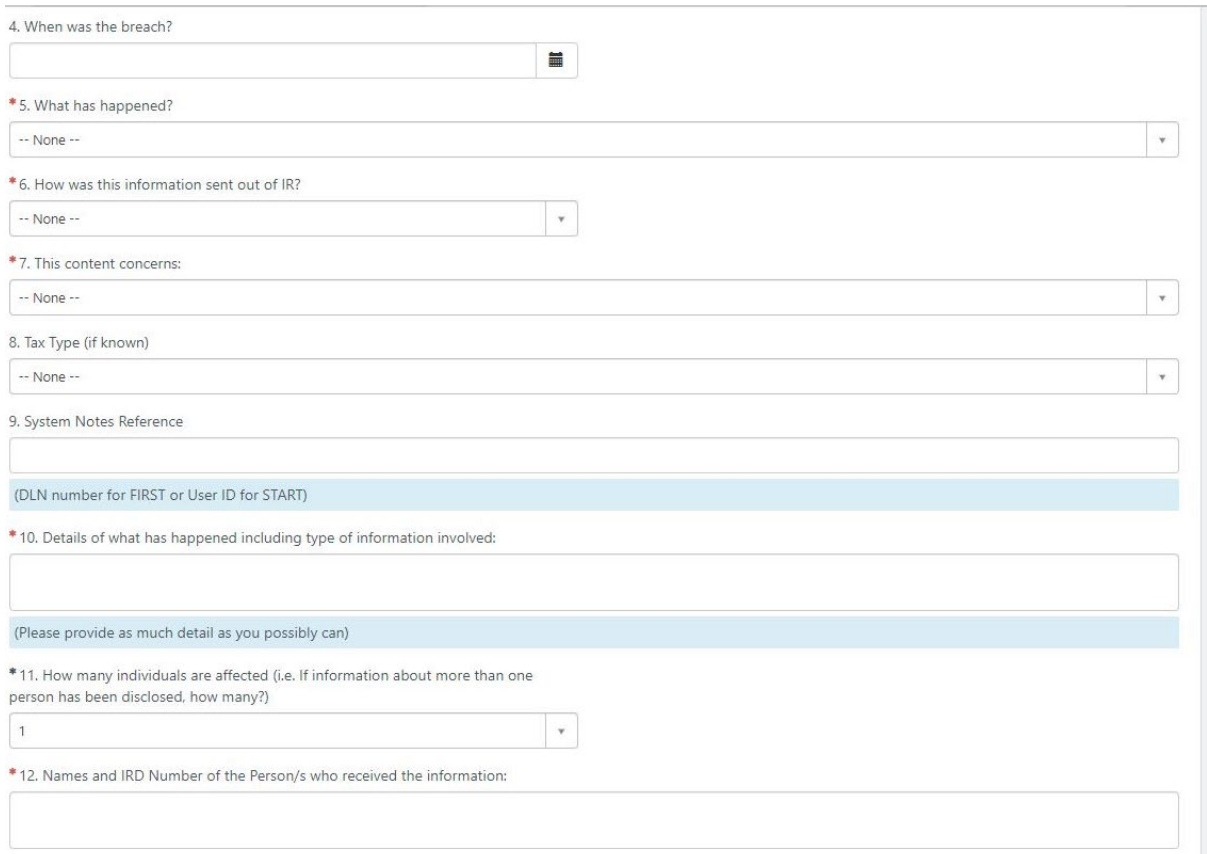
7 Appendix 1 – Privacy Breach Notification Form Example

- Go to: [privacy breach notification form](#).



The screenshot shows the 'Privacy Breach Notification Form' in the Inland Revenue system. The form is titled 'Privacy Breach Notification Form' and includes a search bar at the top. Below the title, there is a large eye icon and a paragraph explaining the purpose of the form: 'Complete this form if you identify an alleged privacy breach (i.e. personal information has been disclosed or sent to the wrong person). It's really important that we know an incident has happened so we can contain it and try to prevent it happening again. We may ask for more information if we need it from you. If you identify possible wrongdoing or misconduct by an Inland Revenue employee, report this to the Integrity team (Click here)'. Below this, it states: 'The incident process is about ensuring the customer gets the required outcome and information is protected. In cases where someone has opened mail that is not addressed to them, this is **NOT** considered a privacy breach. In these cases please refer to START Help – "Cease or invalidate an address".'

The form is divided into two main sections: 'Contact Details' and 'Breach Details'. The 'Contact Details' section includes fields for '1. Person reporting the breach:' (with a dropdown menu showing 'Tim Grindlay (admin)') and '2. Contact phone number:'. The 'Breach Details' section includes fields for '3. Who discovered the breach?' (with a dropdown menu showing '-- None --') and '4. When was the breach?' (with a date picker).



The continuation of the form shows fields for '4. When was the breach?' (with a date picker), '5. What has happened?' (with a dropdown menu showing '-- None --'), '6. How was this information sent out of IR?' (with a dropdown menu showing '-- None --'), '7. This content concerns:' (with a dropdown menu showing '-- None --'), '8. Tax Type (if known)' (with a dropdown menu showing '-- None --'), '9. System Notes Reference' (with a text input field), '10. Details of what has happened including type of information involved:' (with a text input field), '11. How many individuals are affected (i.e. If information about more than one person has been disclosed, how many?)' (with a dropdown menu showing '1'), and '12. Names and IRD Number of the Person/s who received the information:' (with a text input field).

8 Appendix 2 – Delete documents in TIMG archive

Before account types were moved to START, documents were stored in EDSR. Once the account type was moved to START, the correspondence was issued and viewed in START. Correspondence issued prior to the account type being moved to START can be accessed via the EDSR search in the SAFE portal.

The ability to delete documents from the archive is strictly limited. To request access to delete documents contact Amanda Price at s 9(2)(a)

- Open the [SAFE Portal](#)
- Select "Search EDSR"
- Enter either the "IRD number" or "DLN number" of document
- Select "Search" and results will be displayed.
- Select "View" to open the image of the document
- Select "Close" icon to return to the search results
- Select "Request Deletion" – document will delete overnight

≡
Main

IRD Portal

Hi CATHERINE LEE. Welcome to IRD Portal.

Please select below options:

Search EDSR

Search Physical Records

≡ Search Digital
⚡

IRD Number:

DLN Number: Search

| VIEW | DLN NUMBER | IRD NUMBER | TAX TYPE | FORM ID | DATE RANGE | REVIEW DATE | |
|----------------------|------------|------------|----------|---------|-------------------------------|-------------|------------------|
| View | 1195966315 | 65727676 | NCP | CS10 | From: 4/08/2021 To: 4/08/2046 | 4/08/2046 | Request Deletion |

From: [Communications - IR](#)
To: [Freyberg Building All Users](#)
Subject: Have you seen this USB stick?
Date: Thursday, 14 April 2022 3:58:51 pm
Attachments: [image.png](#)

Kia ora Team Freyberg

This is not an Easter egg hunt but one of our colleagues based in Freyberg lost a USB stick on Tuesday, and we're hoping someone may find it.

It was in its packet and looks a bit like the one below, it also had a couple of Post-It notes attached. If you've seen this USB, and picked it up, please drop it into the Mailroom and perhaps we can swap it for a real Easter egg.

Thanks for your time.

Ngā mihi
Internal Communications team



Lessons Learned USB Incident April 2022

Attendees:

Vanessa Johnson
Karen Whitiskie
Jay Harris
Dawn Swan
Ta'au Savaiinaea
Josh Green
Jo Petrie
Tony Morris
Kirsty Gemmill
Rowan McArthur/Gay Cavill
Catherine Lee
James Barker

Facts of Incident

On Tuesday 12 April 2022 a staff member from Legal Services was transporting a USB stick to the IR Upper Hutt Office to have the data on it saved onto a CD-ROM. The USB stick contained interviews of 10 witnesses in a s 18(c)(i) criminal prosecution case.

The person who is being prosecuted in this case resides in the s 18(c)(i) Prison and so the information needed to be saved onto a CD-ROM as USB sticks are not accepted by the Prison.

The USB Stick was transported within a plastic container, tucked inside a Eastlight file and tied up with string. The USB stick is thought to have been lost either within the FRY building or surrounds. Initially the staff member thought it may have been in his car but this did not appear after an extensive search of the vehicle.

The staff member went from the FRY building down to the Lower Ground and to his car parked at the end of the driveway. He then drove to the prison to drop off the Eastlight file before going to the Upper Hutt Office to have the USB contents transferred to the CD-ROM. He realised that the USB Stick was missing so phoned the FRY Office and was informed that there was a USB Stick on his desk, he assumed this was the missing USB. On return to the FRY office he realised it was not the missing USB stick. The staff member checked with the mailroom at the FRY office to check if they had seen it – no one had.

The USB stick was encrypted, however, the staff member had attached a Yellow Post-it Note to the USB Stick detailing the password (digits), but not the word 'password' written on it. The Post-it note also had two names and phone numbers written on it of Corrections staff members who could be contacted if the staff member had issues accessing the prison.

An Incident Report was lodged by the staff member's Manager on Wednesday 13 April 2022. The Manager was relatively new to IR so did a 'search' within Haukainga to work out what she should do in this situation.

The Incident report was lodged and picked up by Cathie Lee (Business Incidents Team). Cathie Lee made contact with Dawn Swan, Privacy Officer, and they met with the staff member. A follow up email was sent to the staff member asking if they had advised the

Police. The staff member did lodge a report with the Police in relation to the lost USB stick.

Dawn Swan assessed at that time that there was no notifiable privacy breach. She also asked the staff member to advise the two Correction Officers of the Post-it Note information.

Dawn Swan organised for an email to go to all FRY staff asking if they found the USB stick (photo attached of what it looked like with the Post-it notes on) for it to be returned to the FRY Mailroom.

Dawn Swan emailed Cath Atkins and Mary Craig to advise as an FYI that the incident had occurred.

Areas for discussion

Why did incident happen – processes / policies not followed

Process for lodging incident

Assessment of incident

Notifications of incident

Escalation of incident

Information Security Aspects

- Process for saving material onto CD-ROM
- Action Point moved to Lessons Learned: (Jay) Education - Consider how we manage these processes – provide confidence to the public in relation to how we manage information generally. Also consideration with these instances vis a vis the email sent to all FRY staff disclosing that the USB Stick had been lost.
- Action Point moved to Lessons Learned: (Jay) Talked to s 9(2)(a), there were four USB keys, they were all used at the same time, Jay has validated that. The one we are questioning is the one missing. They still have no evidence of multiple USB sticks being plugged into machines. This will be part of lessons learned. We have a gap in our log management. Three in our possession. Jay still to get duplicate from Legal Services as per earlier action point.
- Confirmed that the key is lost/not in our possession. s 9(2)(h) hasn't hit any media or social media as far as we know.
- Jay ultimately would like all three USB sticks to understand what can be seen or not.
- Action Point moved to Lessons Learned: Jay to contact Neville Winter to understand his actions in relation to the USB Stick access (it was confirmed he used a system 'off the grid' – need to incorporate this into lessons learned conversation).

Legal Processes

- Who owns the s 18(c)(i) and considers risks from an end to end perspective

From: [Cath Atkins](#)
To: [Karen Whitiskie](#)
Subject: FW: Lessons Learned for USB Stick Incident - Person from the Compliance Area
Date: Wednesday, 27 April 2022 4:59:17 pm
Attachments: [image001.png](#)

[UNCLASSIFIED]

Any thoughts on who you work with most from the compliance area on this stuff? Trevour?

Noho ora mai

Cath Atkins([she/her](#))

Deputy Commissioner Customer & Compliance Services - Business | Inland Revenue Ratonga
Kiritaki Me te Tautukunga - Pakihi | Te Tari Taake

s 9(2)(a) PO Box 2198 | Wellington



From: Joanne Petrie

Sent: Wednesday, 27 April 2022 4:02 pm

To: Cath Atkins

Cc: Vanessa Johnson ; Karen Whitiskie

Subject: Lessons Learned for USB Stick Incident - Person from the Compliance Area

[UNCLASSIFIED]

Kia ora Cath

We are holding a lessons learned session next Tuesday in relation not the USB Stick incident and Naomi has asked for someone to be present from the Compliance area. This is to cover off who manages 'sensitive inquiries' from end to end and considers risks. Could you please advise who should be invited to cover this off?

I look forward to hearing from you.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)



From: [Cath Atkins](#)
To: [Joanne Petrie](#)
Cc: [Vanessa Johnson](#); [Karen Whitiskie](#)
Subject: RE: Lessons Learned for USB Stick Incident - Person from the Compliance Area
Date: Wednesday, 27 April 2022 5:10:51 pm
Attachments: [image001.png](#)

[UNCLASSIFIED]

Hi Jo

Good idea. I have talked to Karen and she is going to come back to you with an appropriate person once she has spoken to Tony. I am on leave thurs/friday. I also had a good chat to Venessa today to catch up with this.

Noho ora mai

Cath Atkins([she/her](#))

Deputy Commissioner Customer & Compliance Services - Business | Inland Revenue Ratonga
Kiritaki Me te Tautukunga - Pakihi | Te Tari Taake

s 9(2)(a) PO Box 2198 | Wellington



From: Joanne Petrie

Sent: Wednesday, 27 April 2022 4:02 pm

To: Cath Atkins

Cc: Vanessa Johnson ; Karen Whitiskie

Subject: Lessons Learned for USB Stick Incident - Person from the Compliance Area

[UNCLASSIFIED]

Kia ora Cath

We are holding a lessons learned session next Tuesday in relation not the USB Stick incident and Naomi has asked for someone to be present from the Compliance area. This is to cover off who manages 'sensitive inquiries' from end to end and considers risks. Could you please advise who should be invited to cover this off?

I look forward to hearing from you.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)



From: [James Barker](#)
To: [Vanessa Johnson](#); [Jay Harris](#); [Tony Morris](#); [Dawn Swan](#); [Catherine Lee](#); [Joanne Petrie](#); [Josh Green](#); [Kirsty Gemmill](#); [Karen Whitiskie](#); [Rowan McArthur](#); [Gay Cavill](#); [Ta'au Savaiinaea](#)
Cc: [Paul Le Sueur](#)
Subject: FW: Lessons Learned - USB Incident April 2022 (002)
Date: Thursday, 12 May 2022 7:43:52 am
Attachments: [Privacy Breach Operating Manual \(v4\).docx](#)

Hi all,
With Catherine's help we asked Paul what he might be able to find from Pou Whirinaki. He has searched old folders and couldn't find what Charlene had completed but he did have this, page 14 includes a process map on incident management that could be a solid starting point for a refresh on roles and accountabilities.
Thanks, James

From: Joanne Petrie s 9(2)(a)
Sent: Tuesday, 3 May 2022 12:58 PM
To: Vanessa Johnson s 9(2)(a); Jay Harris s 9(2)(a); Tony Morris s 9(2)(a); Dawn Swan s 9(2)(a); Catherine Lee s 9(2)(a); James Barker s 9(2)(a); Josh Green s 9(2)(a); Kirsty Gemmill s 9(2)(a); Karen Whitiskie s 9(2)(a); Rowan McArthur s 9(2)(a); Gay Cavill s 9(2)(a); Ta'au Savaiinaea s 9(2)(a)
Subject: Lessons Learned - USB Incident April 2022 (002)
[UNCLASSIFIED]

Kia ora koutou
Please find attached the outline for today's lessons learned session.
Nga mihi
Jo

From: [Joanne Petrie](#)
To: [Vanessa Johnson](#)
Cc: [Karen Whitiskie](#)
Subject: DRAFT Lessons Learned - USB Incident April 2022 (002)
Date: Thursday, 19 May 2022 2:22:45 pm
Attachments: [Lessons Learned - USB Incident April 2022 \(002\).docx](#)

[UNCLASSIFIED]

Kia ora

I'm not sure when you'll get a chance to look at this but wanted to get it through to you for review.

Please let me know if you would like each area captured differently etc.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

Lessons Learned USB Incident April 2022

Attendees:

Vanessa Johnson, Service Lead, Integrity & Internal Assurance
Karen Whitiskie, Legal Services Leader
Jay Harris, Chief Information Security Officer
Dawn Swan, Privacy Officer
Josh Green, Domain Lead, Governance & Ministerial Services
Jo Petrie, Management Support to CE & DC, ED&I & Team Lead – Executive Services
Tony Morris, Customer Segment Leader, Significant Enterprises
Kirsty Gemmill, Service Leader, Governance, Ministerial & Executive Services
Gay Cavill, Domain Principal, Marketing & Communications
Catherine Lee, Capability & Outcomes Specialist
James Barker, Domain Lead, Operational Support
Ta'au Savaiinaea, Domain Specialist, Integrity (*apologies*)

Facts of Incident

On Tuesday 12 April 2022 a staff member from Legal Services was transporting a USB stick to the IR Upper Hutt Office to have the data on it saved onto a CD-ROM. The USB stick contained 10 interviews of 9 witnesses in a s 18(c)(i) criminal prosecution case.

The person who is being prosecuted in this case resides in the s 18(c)(i) Prison and so the information needed to be saved onto a CD-ROM as USB sticks are not accepted by the Prison.

The USB Stick was transported within its plastic container, tucked inside a Eastlight file and tied up with string. The USB stick is thought to have been lost either within the FRY building or surrounds. Initially the staff member thought it may have been in his car, but this did not appear to be the case after an extensive search of the vehicle.

The staff member went from the FRY building down to the Lower Ground and to his car parked at the end of the driveway. He then drove to the prison to drop off the Eastlight file before going to the Upper Hutt Office to have the USB contents transferred to the CD-ROM. He realised that the USB Stick was missing so phoned the FRY Office and was informed that there was a USB Stick on his desk, he assumed this was the missing USB. On return to the FRY office he realised it was not the missing USB stick. The staff member checked with the mailroom at the FRY office to check if they had seen it – no one had.

The USB stick was encrypted, however, the staff member had attached a Yellow Post-it Note to the USB Stick detailing the password (digits), but not the word 'password' written on it. The Post-it note also had two names and phone numbers written on it of Corrections staff members who could be contacted if the staff member had issues accessing the prison.

An Incident Report was lodged by the staff member after being advised the reporting process by his Manager on Wednesday 13 April 2022. The Manager was relatively new to IR so did a 'search' within Haukainga to work out what she should do in this situation.

The Incident report was lodged and picked up by Cathie Lee (Business Incidents Team). Cathie Lee made contact with Dawn Swan, Privacy Officer, and they met with the staff member. A follow up email was sent to the staff member asking if they had advised the Police. The staff member did lodge a report with the Police in relation to the lost USB stick.

Dawn Swan assessed at that time that there was no notifiable privacy breach. She discussed advising the two Correction Officers of the Post-it Note information.

Dawn Swan organised for an email to go to all FRY staff asking if they found the USB stick (photo attached of what it looked like with the Post-it notes on) for it to be returned to the FRY Mailroom.

Dawn Swan emailed Cath Atkins and Mary Craig to advise as an FYI that the incident had occurred.

Areas for discussion

Why did incident happen – processes / policies not followed

The following was confirmed:

- Using a USB key to transfer information in these circumstances is relatively common. The process around transferring the information was followed.
- The process for Legal Services transporting/moving information/documents is to use a briefing/case with a padlock.

Actions as a result:

- The instructions when using a USB stick are being reviewed by Karen.
- Business Management Checks will include a check on these instructions being used.
- These instructions will be included in the Induction Process for all Legal Services staff.
- CISO/Legal Services and Digital Forensics will review the USB Policy and once finalised user education will follow. Review of the Password Policy is currently underway and is due to be issued soon so this can be dovetailed into the user education.
- CISO - Work is underway in relation to the exemptions process with a view to individual exemptions being provided and 'blanket' exemptions will no longer be available. Leader education to be provided in relation to what is agreed in relation to exemptions and what will be required.
- Ross Walker (Security) - the Transportation Policy is to be updated. The Policy needs to cover what process is to be followed when only transporting one item. Visibility of the updated Policy and education as appropriate will be required for anyone in CCS who carries documents. Consideration also to be given for this Policy from an enterprise wide perspective not just within CCS.

Process for lodging incident; assessment of incident; notifications of incident; escalation of incident

The following was confirmed:

The tool used in this instance to lodge the incident was focussed on reporting a privacy breach. ServiceNow was confirmed as the tool to lodge any other type of incident. The workflow from ServiceNow results in any incident being managed by the respective business area. The Operations Team who manage privacy breach incidents do not have visibility of other incidents.

Consideration needs to be made on how all incidents are managed so there is a clear understanding of what the incident is. Noting that whilst it is ok for business units to manage the incident there might be a wider theme coming through from an enterprise level. Using technology to workflow incidents works well but this misses the human element of looking for any potential wider impacts that may potentially exist. There is also an element of consideration around incidents and when they may evolve and should be managed by our Crisis Management mechanism. There had been a process in place

previously for managing incidents but it was not clear if this was being used. It is unclear who the 'Business Owner' is for incidents.

Actions as a result:

- Legal Services Leaders have been advised on how to lodge an incident/breach.
- James – Operational Support – source the process which was established post Pou Whirinaki in relation to the business managing incidents.
- The business incident process in general needs to be reviewed. Key areas for consideration in managing an incident are noted as:
 - A facilitator role is required in working through the incident
 - Is there a role for SPS in managing incidents?
 - Is it the role of Strategic Advisors to apply some judgment on next steps etc in relation to managing an incident, consider possible impacts, reputation risk and then for a War Room to be created to manage the incident?
 - Where are the escalation points and also who has visibility of when an incident is lodged?

Information Security Aspects

General:

IR is responsible for providing confidence to the public in relation to how we manage information generally.

It was noted that the work completed/accessed etc by the Digital Forensics area is unable to be reviewed/access by Cyber Security. Consideration should be given on this aspect going forward.

Actions as a result:

- CISO – consider the current process used with transferring audio files from a USB stick to a CD-ROM. Explore alternative options of doing this. Consider if there is a different process for documents vs audio files. Validate if there is a better way of managing this process without USB sticks.
- CISO/CyberSecurity – to complete a detail log review of the USB stick.
- CISO – consider options for wiping a USB stick if it is lost/unaccounted for.
- All USB sticks are to be individually numbered and any existing sticks 'cleansed'.
- CISO - weave updates and messages as a result of this lessons learned into the Education Awareness Programme.

Legal Processes - Who owns the s 18(c)(i) and considers risks from an end to end perspective

The following was confirmed:

- With changes in the org design the responsibility of a case from end to end has changed. In the past a case would have remained under the control of the compliance officer ('the case officer') and their leader and when it moved to prosecution then the case officer would have taken a step back as it was not their area of expertise but they would still have been responsible for assessing the overall risk.
- Legal Services did have certain precautions in place with this individual case and confirmed that Legal Services was more involved in meetings etc given the individual.

Actions as a result:

- Tony/Karen - It is necessary to reinforce the 'Case Officer' role. This role/aspect will be reviewed and then consideration around clarifying this role in the new structure.
- Create a process within case management where if certain aspects of the case are triggered e.g. information needs to be transferred to a CD-ROM), then there is an expert in this field identified for the staff member to seek advice/confirm the process.

- Integrity – working from home aspect of not having someone perhaps on hand to check on process etc – consider how checking in can be weaved into other communications/education we do.

DRAFT

From: [Joanne Petrie](#)
To: [Karen Whitiskie](#); [Dawn Swan](#); [Jay Harris](#)
Cc: [Vanessa Johnson](#)
Subject: Clarity for Lessons Learned document
Date: Thursday, 26 May 2022 3:12:54 pm

Kia ora koutou

I'm just finalising the Lessons Learned document in relation to the USB stick and Vanessa had a few points of clarification before I do so and distribute. Could you please respond to me on the queries allocated to you:

Karen:

- Could you please advise if the "USB stick containing 10 interviews of 9 witnesses" included an interview with the defendant?
- "Ross Walker (Security) - the Transportation Policy is to be updated. The Policy needs to cover what process is to be followed when only transporting one item. Visibility of the updated Policy and education as appropriate will be required for anyone in CCS who carries documents. Consideration also to be given for this Policy from an all of IR perspective not just within CCS." – Is this Policy currently more CCS focussed?

Jay/Karen:

- "CISO/Legal Services and Digital Forensics will review the USB Policy and once finalised user education will follow." - Was this just relating to LS or all of IR? Vanessa thinks this was more related to looking at a smarter / safer way to provide the DJ unit access to the information to be burnt onto disc – can you please clarify?

Jay:

- "All USB sticks are to be individually numbered and any existing sticks 'cleansed'." – Vanessa: I am not sure how this would happen as a number of us hold USBs etc. Perhaps it should be a recall of all USBs not currently covered under an exemption etc – owned by CISO – please clarify

Dawn:

- "The staff member did lodge a report with the Police in relation to the lost USB stick." – does the staff member need to do anything in terms of follow up with the Police in terms of the complaint he made?

I look forward to hearing from you.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198


Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

PO Box 2198
Level 4 Asteron Centre
55 Featherston Street
WELLINGTON 6011
s 9(2)(a)

A grey rectangular redaction box covering the text 's 9(2)(a)' and extending to the right.

Leilana Walker

From: Joanne Petrie
Sent: Thursday, 2 June 2022 3:33 pm
To: Jay Harris; Karen Whitiskie; Dawn Swan
Cc: Vanessa Johnson
Subject: RE: Clarity for Lessons Learned document

[UNCLASSIFIED]

Great, many thanks Jay for clarifying. I will now give Vanessa the final final and get this out and share it with ELT?

From: Jay Harris
Sent: Thursday, 2 June 2022 3:19 pm
To: Joanne Petrie ; Karen Whitiskie ; Dawn Swan
Cc: Vanessa Johnson
Subject: RE: Clarity for Lessons Learned document

[UNCLASSIFIED]

Hi Jo,

Thanks for the reminder/prompt. Please see my responses below in [Blue](#).

From: Joanne Petrie s 9(2)(a)
Sent: Thursday, 2 June 2022 2:16 PM
To: Karen Whitiskie s 9(2)(a) ; Dawn Swan s 9(2)(a) ; Jay Harris s 9(2)(a)
Cc: Vanessa Johnson s 9(2)(a)
Subject: RE: Clarity for Lessons Learned document

[UNCLASSIFIED]

Kia ora Jay

Just following up on my original request for clarification so I can look to finalise the Lessons Learned for this incident.

I look forward to hearing from you.

Nga mihi
jo

From: Karen Whitiskie s 9(2)(a)
Sent: Sunday, 29 May 2022 2:25 pm
To: Joanne Petrie s 9(2)(a) ; Dawn Swan s 9(2)(a) ; Jay Harris s 9(2)(a)
Cc: Vanessa Johnson s 9(2)(a)
Subject: RE: Clarity for Lessons Learned document

Hi

Please see my comments in red below.

Thanks

Karen

From: Joanne Petrie s 9(2)(a)
Sent: Thursday, 26 May 2022 3:13 PM
To: Karen Whitiskie s 9(2)(a); Dawn Swan s 9(2)(a); Jay Harris s 9(2)(a)
Cc: Vanessa Johnson s 9(2)(a)
Subject: Clarity for Lessons Learned document

[UNCLASSIFIED]

Kia ora koutou

I'm just finalising the Lessons Learned document in relation to the USB stick and Vanessa had a few points of clarification before I do so and distribute. Could you please respond to me on the queries allocated to you:

Karen:

- Could you please advise if the "USB stick containing 10 interviews of 9 witnesses" included an interview with the defendant? **Yes this included an interview with the defendant.**
- "Ross Walker (Security) - the Transportation Policy is to be updated. The Policy needs to cover what process is to be followed when only transporting one item. Visibility of the updated Policy and education as appropriate will be required for anyone in CCS who carries documents. Consideration also to be given for this Policy from an all of IR perspective not just within CCS."
 - Is this Policy currently more CCS focussed? **Yes the current policy is CCS focused. I have asked Eteline Tiraa to follow up with Ross around a new policy.**

Jay/Karen:

- "CISO/Legal Services and Digital Forensics will review the USB Policy and once finalised user education will follow." - Was this just relating to LS or all of IR? Vanessa thinks this was more related to looking at a smarter / safer way to provide the DJ unit access to the information to be burnt onto disc – can you please clarify? **This was both LS and all of IR. LS is updating our current policy as an interim measure while the wider IR work Jay is doing is done. If Jay can find a better way than using USB's I am all for it. This was/will be across all of IR. Vanessa's memory is related to my next response below. Actions underway or completed are that we have reviewed all USB exemptions (including blanket ones) and gone to each individual to validate their need for one. We now have an individualised list of USB exemptions with expiry dates to be monitored. We are also including the USB usage topic as part of our ongoing awareness campaigns/comms.**

Jay:

- "All USB sticks are to be individually numbered and any existing sticks 'cleansed'." – Vanessa: I am not sure how this would happen as a number of us hold USBs etc. Perhaps it should be a recall of all USBs not currently covered under an exemption etc – owned by CISO – please clarify **This is in relation to how we can define a smarter/safer way of using USBs. There are several options we are exploring including issuing USB's, forcing encryption, date bound encryption (if it exists) and unique identifiers for USB keys. An easy, short-term solution might be to have a department i.e. LS, inventory existing keys held by their exempted personnel and then manually, uniquely identify them (key 1 thru x) with a "check-in, check-out" system in place.**

Dawn:

- "The staff member did lodge a report with the Police in relation to the lost USB stick." – does the staff member need to do anything in terms of follow up with the Police in terms of the complaint he made? **I wouldn't have thought so as this was a lost property report.**

I look forward to hearing from you.

Nga mihi
Jo

Jo Petrie
Team Lead & Management Support (CE & DC ED&I) – Executive Services
Enterprise Design & Integrity
Inland Revenue
PO Box 2198
Level 4 Asteron Centre
55 Featherston Street
WELLINGTON 6011
s 9(2)(a)

**Lessons Learned
USB Incident
April 2022
Actions – Internal Assurance**

| Number | Action | Owner | Completion Date |
|--|--|-----------------|------------------------|
| <i>Why did incident happen – processes / policies not followed</i> | | | |
| 1 | Legal Services instructions when using a USB stick are being reviewed by Karen. | Karen Whitiskie | |
| 2 | Business Management Checks will include a check on these instructions being followed. | Karen Whitiskie | |
| 3 | USB instructions will be included in the Induction Process for all Legal Services staff. | Karen Whitiskie | |
| 4 | CISO/Legal Services and Digital Forensics will review the USB Policy and once finalised user education will follow. | Jay Harris | |
| 5 | Review of IR's Password Policy is currently underway and is due to be issued soon so this can be dovetailed into the user education. | Jay Harris | |
| 6 | CISO - Work is underway in relation to the exemptions process with a view to individual exemptions being provided and 'blanket' exemptions will no longer be available. Leader education to be provided in relation to what is agreed in relation to exemptions and what will be required. | Jay Harris | |
| 7 | The Transportation Policy is to be updated. The Policy needs to cover what process is to be followed when only transporting one item. The current Policy is CCS focussed so a new Policy needs to be created for all staff who carry documents. | Ross Walker | |
| <i>Process for lodging incident; assessment of incident; notifications of incident; escalation of incident</i> | | | |
| 8 | Legal Services Leaders have been advised on how to lodge an incident/breach. | Karen Whitiskie | |
| 9 | Operational Support – to source the process which was established by Pou Whirinaki in relation to the business managing incidents. | James Barker | |

| | | | |
|--|---|-----------------------------|--|
| 10 | <ul style="list-style-type: none"> - The business incident process in general needs to be reviewed. Key areas for consideration in managing an incident are noted as: <ul style="list-style-type: none"> - A facilitator role is required in working through the incident - Is there a role for the Strategic Portfolio Stewardship team in managing business incidents? - Is it the role of Strategic Advisors to apply some judgment on next steps etc in relation to managing an incident, consider possible impacts, reputation risk and then for a War Room to be created to manage the incident? - Where are the escalation points and also who has visibility of when an incident is lodged? | Vanessa/Mary Craig? | |
| <i>Information Security Aspects</i> | | | |
| 11 | Consider the current process used with transferring audio files from a USB stick to a CD-ROM. Explore alternative options of doing this. Consider if there is a different process for documents vs audio files. Validate if there is a better way of managing this process without USB sticks. | Jay Harris | |
| 12 | To complete a review of IR's process to monitor and log actual use of USBs on individual devices. | Jay Harris/Michael Tench | |
| 13 | Consider options for wiping a USB stick if it is lost/unaccounted for. | Jay Harris | |
| 14 | All USB sticks are to be individually numbered and any existing sticks 'cleansed'. | Jay Harris | |
| 15 | Weave updates and messages as a result of this lessons learned into the Education Awareness Programme. | Jay Harris | |
| <i>Legal Processes - Who owns the high-profile prosecutions process and considers risks from an end to end perspective</i> | | | |
| 16 | It is necessary to reinforce the 'Case Officer' role. This role/aspect will be reviewed and then consideration around clarifying this role in the new structure. | Tony Morris/Karen Whitiskie | |
| 17 | Create a process within case management where if certain aspects of the case are triggered e.g. information needs to be transferred to a CD-ROM), then there is an expert in this field | Jay Harris? | |

| | | | |
|----|--|--------------|--|
| | identified for the staff member to seek advice/confirm the process. | | |
| 18 | Working from home aspect of not having someone perhaps on hand to check on process etc – consider how checking in can be weaved into other communications/education we do. | Chris Linton | |

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: RE: Action Points from Lessons Learned
Date: Friday, 17 June 2022 11:24:54 am

All good – not really sure I understand AP 16?
Otherwise 1 should nearly be finalised subject to final comments on what I sent out yesterday.
This can then be included as part of ongoing induction. Re point 8 the instructions for this can
shared with the finalised USB process to all leaders.

From: Karen Whitiskie
Sent: Friday, 17 June 2022 9:24 AM
To: Eteline Tiraa
Subject: FW: Action Points from Lessons Learned

Hi Eteline

These are my action points but I still need to get my head around what is required.

Karen

Not in scope, Duplicate



From: [Joanne Petrie](#)
To: [Karen Whitiskie](#)
Subject: RE: Action Points from Lessons Learned
Date: Tuesday, 26 July 2022 2:30:41 pm

Kia ora

I'll update point 8 to be completed as I believe you used a team meeting to give visibility to your leaders on the process and yes joining the dots e.g. advising your one up Manager

Nga mihi

Jo

From: Karen Whitiskie
Sent: Monday, 11 July 2022 2:45 pm
To: Joanne Petrie
Subject: RE: Action Points from Lessons Learned

Hi Jo

Apologies for not getting back to you on this sooner.

My action points 1 to 3 are in train. We are in the final checking stage of our revised policy – we just need to hear back from Jay. Once that is finalised 2 and 3 will be ready to go. They should be done by the end of July.

Are you able to clarify action point 8. The right lodging process was used for the USB loss, it was just more the joining of the dots?

Thanks

Karen

From: Joanne Petrie s 9(2)(a)
Sent: Thursday, 23 June 2022 3:15 PM
To: Vanessa Johnson s 9(2)(a); Jay Harris s 9(2)(a); Karen Whitiskie s 9(2)(a); James Barker s 9(2)(a); Chris Linton s 9(2)(a); Ta'au Savaiinaea s 9(2)(a)
Cc: Grant Hunt s 9(2)(a)
Subject: RE: Action Points from Lessons Learned

Kia ora koutou

Just following up on this email and asking you to provide potential completion date or if completed and I can then send this to Grant.

I look forward to hearing from you – have a great Matariki.

Nga mihi

Jo

From: Joanne Petrie s 9(2)(a)
Sent: Monday, 13 June 2022 2:04 pm
To: Vanessa Johnson s 9(2)(a); Jay Harris s 9(2)(a); Karen Whitiskie s 9(2)(a); James Barker s 9(2)(a); Chris Linton s 9(2)(a); Ta'au Savaiinaea s 9(2)(a)
Cc: Grant Hunt s 9(2)(a)
Subject: Action Points from Lessons Learned

Kia ora

Please find attached the Action Point Register which will go to Grant in Internal Assurance to put into their system. Could you please review the actions allocated to you and give a potential

completion date/date completed and send that to me.

I look forward to hearing from you.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

From: [Vanessa Johnson](#)
To: [Ross Walker](#); [Jay Harris](#); [Karen Whitiskie](#)
Subject: Action Points from Lessons Learned - USB Incident April 2022 (002)
Date: Wednesday, 27 July 2022 9:31:38 am
Attachments: [Action Points from Lessons Learned - USB Incident April 2022 \(002\).docx](#)

Hi everyone

Can I please have an update and planned completion date for your items.

Thanks

Vanessa

**Lessons Learned
USB Incident
April 2022
Actions – Internal Assurance**

| Number | Action | Owner | Completion Date |
|--|--|-----------------|------------------------|
| <i>Why did incident happen – processes / policies not followed</i> | | | |
| 1 | Legal Services instructions when using a USB stick are being reviewed by Karen. | Karen Whitiskie | End of July |
| 2 | Business Management Checks will include a check on these instructions being followed. | Karen Whitiskie | End of July |
| 3 | USB instructions will be included in the Induction Process for all Legal Services staff. | Karen Whitiskie | End of July |
| 4 | CISO/Legal Services and Digital Forensics will review the USB Policy and once finalised user education will follow. | Jay Harris | |
| 5 | Review of IR's Password Policy is currently underway and is due to be issued soon so this can be dovetailed into the user education. | Jay Harris | |
| 6 | CISO - Work is underway in relation to the exemptions process with a view to individual exemptions being provided and 'blanket' exemptions will no longer be available. Leader education to be provided in relation to what is agreed in relation to exemptions and what will be required. | Jay Harris | |
| 7 | The Transportation Policy is to be updated. The Policy needs to cover what process is to be followed when only transporting one item. The current Policy is CCS focussed so a new Policy needs to be created for all staff who carry documents. | Ross Walker | |
| <i>Process for lodging incident; assessment of incident; notifications of incident; escalation of incident</i> | | | |
| 8 | Legal Services Leaders have been advised on how to lodge an incident/breach. | Karen Whitiskie | Completed |
| 9 | Operational Support – to source the process which was established by Pou Whirinaki in relation to the business managing incidents. | James Barker | Unable to locate |

| | | | |
|--|---|-----------------------------|--|
| 10 | <ul style="list-style-type: none"> - The business incident process in general needs to be reviewed. Key areas for consideration in managing an incident are noted as: <ul style="list-style-type: none"> - A facilitator role is required in working through the incident - Is there a role for the Strategic Portfolio Stewardship team in managing business incidents? - Is it the role of Strategic Advisors to apply some judgment on next steps etc in relation to managing an incident, consider possible impacts, reputation risk and then for a War Room to be created to manage the incident? - Where are the escalation points and also who has visibility of when an incident is lodged? | Vanessa/Mary Craig? | <p>Understanding the current process/s and identifying areas for improvement – 31 July 2022</p> <p>Allocating ownership of improvement areas and development of next steps re implementation – 31 August 2022</p> <p>Implementation of changes – TBC</p> |
| <i>Information Security Aspects</i> | | | |
| 11 | Consider the current process used with transferring audio files from a USB stick to a CD-ROM. Explore alternative options of doing this. Consider if there is a different process for documents vs audio files. Validate if there is a better way of managing this process without USB sticks. | Jay Harris | |
| 12 | To complete a review of IR's process to monitor and log actual use of USBs on individual devices. | Jay Harris/Michael Tench | |
| 13 | Consider options for wiping a USB stick if it is lost/unaccounted for. | Jay Harris | |
| 14 | All USB sticks are to be individually numbered and any existing sticks 'cleansed'. | Jay Harris | |
| 15 | Weave updates and messages as a result of this lessons learned into the Education Awareness Programme. | Jay Harris | |
| <i>Legal Processes - Who owns the high-profile prosecutions process and considers risks from an end to end perspective</i> | | | |
| 16 | It is necessary to reinforce the 'Case Officer' role. This role/aspect will be reviewed and then consideration around clarifying this role in the new structure. | Tony Morris/Karen Whitiskie | |
| 17 | Create a process within case management where if certain aspects of the case are triggered e.g. information needs to be transferred to a CD-ROM), then there is an expert in this field | Jay Harris? | |

| | | | |
|----|--|--------------|---|
| | identified for the staff member to seek advice/confirm the process. | | |
| 18 | Working from home aspect of not having someone perhaps on hand to check on process etc – consider how checking in can be weaved into other communications/education we do. | Chris Linton | Comms to be woven into Jay's comms/education plan |

From: Valerie Johnson
Sent: Friday, 26 August 2022 10:46 am
To: Karen Whitiskie
Subject: RE: Open Recommendation - Lessons Learned USB Incident

Hi Karen

For a starter I think it could be included in the Induction Workbook we prepare for the newbie. The TL must specifically include this conversation and have a tick box in the checklist when doing the forms perhaps as this is the first thing they do with the team member.

What do you think?

Val.

From: Karen Whitiskie
Sent: Friday, 26 August 2022 10:18 AM
To: Valerie Johnson
Subject: FW: Open Recommendation - Lessons Learned USB Incident

Hi Val

Can you think about how we put the induction part in place?

Thanks

Karen

From: Grant Hunt s 9(2)(a)
Sent: Friday, 26 August 2022 10:16 AM
To: Karen Whitiskie s 9(2)(a)
Subject: RE: Open Recommendation - Lessons Learned USB Incident

Karen thanks for getting back to me so quickly.

Based on your comments that all three items will be completed next week, I will update the database accordingly and they will closed off on the 2 September.

Thanks
Grant

From: Karen Whitiskie s 9(2)(a)
Sent: Friday, 26 August 2022 10:01 AM
To: Grant Hunt s 9(2)(a)
Subject: RE: Open Recommendation - Lessons Learned USB Incident

Hi Grant

We are just incorporating some final comments from the CISO office (Eteline had a follow up discussion with Aiden Roberts yesterday) and will complete all three items at the end of next week. We will discuss the final version of the policy with our wider leadership team on 1 September after which I will send to the entire team. There have been previous discussions on the draft policy. The BMC check will be included from the next BMC check and it will be included in the Induction Process – we are just trying to figure out the best way to do that.

I also have my fingers cross that a cloud solution option will be found in the future to avoid this all together.

Ngā mihi

Karen Whitiskie (*she/her*)

Legal Services Leader | Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: Grant Hunt s 9(2)(a)

Sent: Friday, 26 August 2022 9:44 AM

To: Karen Whitiskie s 9(2)(a)

Subject: Open Recommendation - Lessons Learned USB Incident

Hi Karen,

Still trying to find a solution to the access issues yourself and some users are having getting into the TeamCentral database.

In the meantime, I note there are three actions that were due to be completed at the end of July. See table below.

Can you please confirm by replying to this email, the status of these.

| Recommendation Title | Impact | Progress | Estimated Implementation Date | Im |
|---|-----------|----------|-------------------------------|----|
| 1. Review Legal Services instructions for using a USB stick. | C3 - High | | 31/07/2022 | |
| 2. Include a check that confirms these instructions are being followed in Business Management Checks. | C3 - High | | 31/07/2022 | |
| 3. Include USB instructions in the Induction Process for all Legal Services staff. | C3 - High | | 31/07/2022 | |

Thanks

Grant

Grant Hunt

Domain Specialist - Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance

** Providing Objective Assurance & Advice**

s 9(2)(a)

From: [Joanne Petrie](#)
To: [Cath Atkins](#)
Cc: [Vanessa Johnson](#); [Karen Whitiskie](#)
Subject: Lessons Learned for USB Stick Incident - Person from the Compliance Area
Date: Wednesday, 27 April 2022 4:01:37 pm

[UNCLASSIFIED]

Kia ora Cath

We are holding a lessons learned session next Tuesday in relation not the USB Stick incident and Naomi has asked for someone to be present from the Compliance area. This is to cover off who manages 'sensitive inquiries' from end to end and considers risks. Could you please advise who should be invited to cover this off?

I look forward to hearing from you.

Nga mihi

Jo

Jo Petrie

Team Lead & Management Support (CE & DC ED&I) – Executive Services

Enterprise Design & Integrity

Inland Revenue

PO Box 2198

Level 4 Asteron Centre

55 Featherston Street

WELLINGTON 6011

s 9(2)(a)

Appendix D

From: [Vanessa Johnson](#)
To: [Dawn Swan](#); [Conrad Bace](#); [Karen Whitiskie](#); [Joanne Petrie](#); [Gay Cavill](#); [Josh Green](#)
Subject: Draft Notification Letter (CB)
Date: Thursday, 28 April 2022 1:22:13 pm
Attachments: [Draft Notification Letter \(CB\).docx](#)

[IN CONFIDENCE RELEASE EXTERNAL]

Hi everyone

I have added in one question re the CD. I just want to ensure we have the correct information as we go through the internal review process as well.

Regards

Vanessa

From: [Gay Cavill](#)
To: [Joanne Petrie](#); [Karen Whitiskie](#); [Vanessa Johnson](#); [Josh Green](#); [Dawn Swan](#); [Conrad Bace](#)
Cc: [Rowan McArthur](#); [Kirsty Gemmill](#)
Subject: FW: USB incident - notification
Date: Thursday, 28 April 2022 2:05:09 pm
Attachments: [image001.png](#)

Here is a draft reactive media response on this matter, **s 9(2)(h)**, that we could use to respond if/when we get media queries on the lost USB.

There is also the question of whether we wait until we get queries or front foot it and put this out as a media release. There are reasons for going proactive which I can outline at this afternoon's meeting.

In the meantime, here is the draft response for you to look at.

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that the information on it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

*If any member of the public finds this USB or already has it in their possession Inland Revenue - no questions asked. **Best way to do that?????***

Regards,
Gay.

From: Gay Cavill
Sent: Thursday, 28 April 2022 1:59 pm
To: **s 9(2)(h)**
Cc: Rowan McArthur ; Dawn Swan ; Josh Green
Subject: RE: USB incident - notification

s 9(2)(h) I will distribute them to the meeting members ahead of the meeting.

There is also another decision to be made – do we wait until we get queries or do we front foot it, put it out as a media release and control the release of the narrative. That has the added bonus of us being open, transparent and showing we realise this is not good.

Reactive media response on the loss of the USB of evidence

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that the information on it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.


To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

*If any member of the public finds this USB or already has it in their possession Inland Revenue - no questions asked. **Best way to do that?????***

s 9(2)(h)

s 9(2)(g)(i), s 9(2)(h)



From: Dawn Swan s 9(2)(a)

Sent: Thursday, 28 April 2022 11:22 am

To: Karen Whitiskie s 9(2)(a) Vanessa Johnson

ss 9(2)(a) Joanne Petrie s 9(2)(a) Gay Cavill

s 9(2)(a) Josh Green ss 9(2)(a) Conrad Bace

s 9(2)(a)

Subject: USB incident - notification

Hi all

We have decided to notify the individuals affected by this incident and so I attach a draft letter that contains the detail expected in this type of notification.

The third page is a draft notification to the two Corrections staff also.

We will have to do a separate letter for the defendant as we may want to include further information. Karen do you want to manage the content for that letter?

We can discuss later this afternoon.

Dawn Swan

Privacy Officer | Enterprise Design & Integrity | Inland Revenue

Asteron Centre, 55 Featherston Street, Wellington

PO Box 2198, Wellington 6140



[Call/chat with me in Teams](#) or s 9(2)(a)

From: [Dawn Swan](#)
To: [Karen Whitiskie](#); [Conrad Bace](#); [Vanessa Johnson](#); [Joanne Petrie](#); [Gay Cavill](#); [Josh Green](#)
Subject: RE: USB incident - notification
Date: Thursday, 28 April 2022 3:38:23 pm
Attachments: [Draft Notification Letter \(003\).docx](#)
[image001.png](#)

And here's the updated version incorporating the feedback.

From: Karen Whitiskie
Sent: Thursday, 28 April 2022 2:33 PM
To: Conrad Bace ; Dawn Swan ; Vanessa Johnson ; Joanne Petrie ; Gay Cavill ; Josh Green
Subject: RE: USB incident - notification

Hi

Here are some comments ahead of our meeting.

s 9(2)(h)

Thanks

Karen

s 9(2)(h)

From: Dawn Swan s 9(2)(a)

Sent: Thursday, 28 April 2022 11:22 AM

To: Karen Whitiskie ss 9(2)(a) Vanessa Johnson

s 9(2)(a) Joanne Petrie ss 9(2)(a) Gay Cavill

s 9(2)(a) Josh Green s 9(2)(a) Conrad Bace

s 9(2)(a)

Subject: USB incident - notification

Hi all

We have decided to notify the individuals affected by this incident and so I attach a draft letter that contains the detail expected in this type of notification.

The third page is a draft notification to the two Corrections staff also.

We will have to do a separate letter for the defendant as we may want to include further information. Karen do you want to manage the content for that letter?

We can discuss later this afternoon.

[Dawn Swan](#)

Privacy Officer | Enterprise Design & Integrity | Inland Revenue

Asteron Centre, 55 Featherston Street, Wellington

PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or s 9(2)(a)

From: Vanessa Johnson
Sent: Thursday, 28 April 2022 1:01 pm
To: Dawn Swan; Karen Whitiskie; Joanne Petrie; Gay Cavill; Josh Green; Conrad Bace
Subject: RE: USB incident - notification

Hi

Do we have to include all the detail currently there?

Vanessa

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue

s 9(2)(a)

From: Dawn Swan
Sent: Thursday, 28 April 2022 11:22 AM
To: Karen Whitiskie ; Vanessa Johnson ; Joanne Petrie ; Gay Cavill ; Josh Green ; Conrad Bace
Subject: USB incident - notification

Hi all

We have decided to notify the individuals affected by this incident and so I attach a draft letter that contains the detail expected in this type of notification.

The third page is a draft notification to the two Corrections staff also.

We will have to do a separate letter for the defendant as we may want to include further information. Karen do you want to manage the content for that letter?

We can discuss later this afternoon.

Dawn Swan
Privacy Officer | Enterprise Design & Integrity | Inland Revenue
Asteron Centre, 55 Featherston Street, Wellington
PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or s 9(2)(a)

s 9(2)(h)

From: Dawn Swan
Sent: Thursday, 28 April 2022 11:22 AM
To: Karen Whitiskie ; Vanessa Johnson ; Joanne Petrie ; Gay Cavill ; Josh Green ; Conrad Bace
Subject: USB incident - notification

Hi all

We have decided to notify the individuals affected by this incident and so I attach a draft letter that contains the detail expected in this type of notification.

The third page is a draft notification to the two Corrections staff also.

We will have to do a separate letter for the defendant as we may want to include further information. Karen do you want to manage the content for that letter?

We can discuss later this afternoon.

Dawn Swan
Privacy Officer | Enterprise Design & Integrity | Inland Revenue
Asteron Centre, 55 Featherston Street, Wellington
PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or s 9(2)(a)

From: Gay Cavill
Sent: Thursday, 28 April 2022 2:24 pm
To: Joanne Petrie; Karen Whitiskie; Vanessa Johnson; Josh Green; Dawn Swan; Conrad Bace
Cc: Rowan McArthur; Kirsty Gemmill
Subject: RE: USB incident - notification

Slight amendments to this – should read:

Reactive media response on the loss of the USB of evidence

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We have notified those directly affected. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

*If any member of the public finds this USB or already has it in their possession please return it to Inland Revenue - no questions asked. **Best way to do that?????***

From: Gay Cavill
Sent: Thursday, 28 April 2022 2:05 pm
To: Joanne Petrie ; Karen Whitiskie ; Vanessa Johnson ; Josh Green ; Dawn Swan ; Conrad Bace

Cc: Rowan McArthur ; Kirsty Gemmill
Subject: FW: USB incident - notification

Here is a draft reactive media response on this matter, s 9(2)(h), that we could use to respond if/when we get media queries on the lost USB.

There is also the question of whether we wait until we get queries or front foot it and put this out as a media release. There are reasons for going proactive which I can outline at this afternoon's meeting.

In the meantime, here is the draft response for you to look at.

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that the information on it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

If any member of the public finds this USB or already has it in their possession Inland Revenue - no questions asked.

Best way to do that?????

Regards,

Gay.

From: Gay Cavill

Sent: Thursday, 28 April 2022 1:59 pm

To: s 9(2)(h) s 9(2)(a)

Cc: Rowan McArthur ss 9(2)(a) Dawn Swan ss 9(2)(a) Josh Green

s 9(2)(a)

Subject: RE: USB incident - notification

s 9(2)(h)

I will distribute them to the meeting members ahead of the meeting.

There is also another decision to be made – do we wait until we get queries or do we front foot it, put it out as a media release and control the release of the narrative. That has the added bonus of us being open, transparent and showing we realise this is not good.

Reactive media response on the loss of the USB of evidence

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that the information on it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

If any member of the public finds this USB or already has it in their possession Inland Revenue - no questions asked.

Best way to do that??????

s 9(2)(h)



From: Dawn Swan s 9(2)(a)
Sent: Thursday, 28 April 2022 11:22 am
To: Karen Whitiskie ss 9(2)(a) Vanessa Johnson ss 9(2)(a) Joanne Petrie s 9(2)(a) Gay Cavill ss 9(2)(a) Josh Green s 9(2)(a) Conrad Bace s 9(2)(a)
Subject: USB incident - notification

Hi all

We have decided to notify the individuals affected by this incident and so I attach a draft letter that contains the detail expected in this type of notification.

The third page is a draft notification to the two Corrections staff also.

We will have to do a separate letter for the defendant as we may want to include further information. Karen do you want to manage the content for that letter?

We can discuss later this afternoon.

Dawn Swan
Privacy Officer | Enterprise Design & Integrity | Inland Revenue
Asteron Centre, 55 Featherston Street, Wellington
PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or s 9(2)(a)

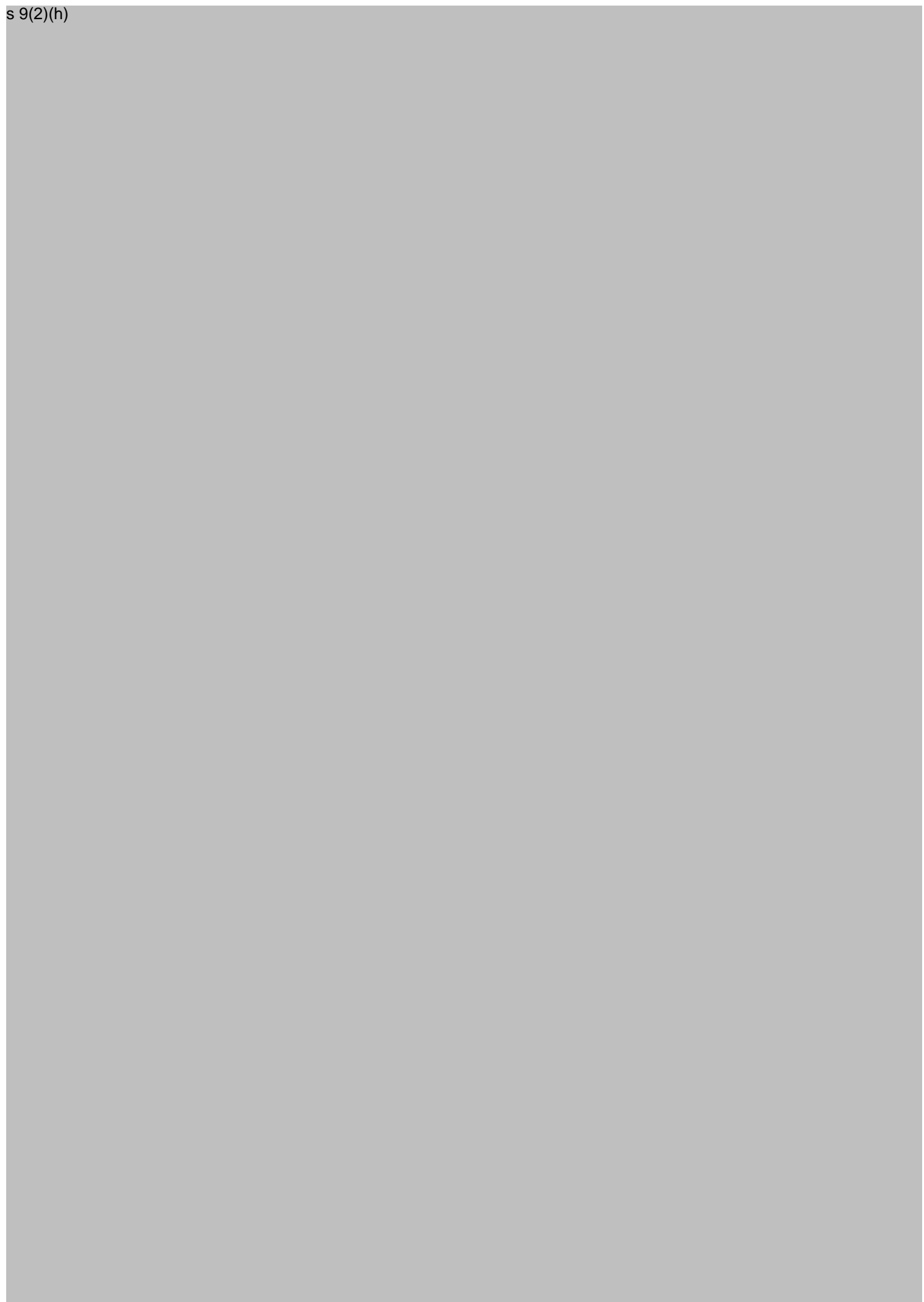
From: [Joanne Petrie](#)
To: [Dawn Swan](#); [Vanessa Johnson](#); [Josh Green](#); [Conrad Bace](#); [Karen Whitiskie](#)
Subject: Draft Notification Letter (003) Clean
Date: Friday, 29 April 2022 8:51:24 am
Attachments: [Draft Notification Letter \(003\) Clean.docx](#)

[IN CONFIDENCE RELEASE EXTERNAL]

Just a couple of bits from me in the attached












s 9(2)(h)

Not in scope, Duplicate

s 18(c)(i)



From: s 9(2)(a)
To: [Karen Whitiskie](#)
Subject: RE: Missing USB - Addresses
Date: Monday, 2 May 2022 12:27:13 pm

Looking deeper I did have the address for both of them. I have just sent you this, might still pay to courier them.

Sorry, I'm not sure if its Ms or Mrs

s 9(2)(a)

From: Karen Whitiskie
Sent: Monday, 2 May 2022 12:20 pm
To: s 9(2)(a)
Subject: RE: Missing USB - Addresses

Also do you happy to know if it is s 18(c)(i)
Don't search START on this – it is just if you know.

From: s 9(2)(a)
Sent: Monday, 2 May 2022 12:07 PM
To: Karen Whitiskie ss 9(2)(a)
Subject: RE: Missing USB - Addresses

Hi Karen,

Do you mean the two Officers that were named on the 'sticky' that was on the missing USB?

I only have their email and phone numbers:

s 18(c)(i)

s 18(c)(i)

s 18(c)(i)

s 18(c)(i)

Do you want their personal addresses? I would need to contact them or look them up in START.

Regards,

s 9(2)(a)

From: Karen Whitiskie ss 9(2)(a)
Sent: Monday, 2 May 2022 11:26 am
To: s 9(2)(a)
Subject: RE: Missing USB - Addresses

Hi

Can you also give me the details of the two Correction officers and the address to send letters to them?

Thanks

Karen

From: s 9(2)(a)
Sent: Monday, 2 May 2022 9:43 AM
To: Karen Whitiskie ss 9(2)(a)
Subject: Missing USB - Addresses

Hi Karen,

These are the relevant addresses

s 18(c)(i)

[Redacted text block]

Regards,

s 9(2)(a)


[Redacted text block]

From: Vanessa Johnson
Sent: Monday, 2 May 2022 1:50 pm
To: Karen Whitiskie; Dawn Swan; Conrad Bace; Josh Green; Gay Cavill; Joanne Petrie
Cc: Rowan McArthur; Kirsty Gemmill; Cath Atkins
Subject: RE: USB incident - notification

Hmmm slightly problematic. Perhaps see if we can find an actual address. If not I suppose we will use the PO box

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue


s 9(2)(a)



From: Karen Whitiskie
Sent: Monday, 2 May 2022 1:47 PM
To: Dawn Swan ; Conrad Bace ; Josh Green ; Gay Cavill ; Joanne Petrie ; Vanessa Johnson
Cc: Rowan McArthur ; Kirsty Gemmill ; Cath Atkins
Subject: RE: USB incident - notification

Dumb question – I assume the one's where we only have a PO BOX or Private Bag address – we won't be able to courier it out?

s 9(2)(h)



s 9(2)(h)

From: Josh Green <s 9(2)(a)>
Sent: Monday, 2 May 2022 10:42 AM
To: Gay Cavill <s 9(2)(a)> Joanne Petrie <s 9(2)(a)> Karen Whitiskie
<s 9(2)(a)> Vanessa Johnson <s 9(2)(a)> Dawn Swan

<s 9(2)(a) Conrad Bace <s 9(2)(a)
Cc: Rowan McArthur <s 9(2)(a) Kirsty Gemmill <s 9(2)(a) Cath Atkins
<s 9(2)(a)
Subject: RE: USB incident - notification

Updates within this meeting below FYI

Thanks

Josh

Reactive media response on the loss of the USB of evidence

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost in transit between two of the department's offices in Wellington. Despite considerable efforts to locate the USB, it hasn't been located.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

We are reviewing our processes in relation to this incident, which is in progress. We anticipate our processes will be adjusted following this incident. This incident has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We have notified those directly affected. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

From: Gay Cavill
Sent: Thursday, 28 April 2022 2:05 pm
To: Joanne Petrie <s 9(2)(a) Karen Whitiskie <s 9(2)(a) Vanessa Johnson
<s 9(2)(a) Josh Green <s 9(2)(a) Dawn Swan <s 9(2)(a)
Conrad Bace <s 9(2)(a)
Cc: Rowan McArthur <s 9(2)(a) Kirsty Gemmill <s 9(2)(a)
Subject: FW: USB incident - notification

Here is a draft reactive media response on this matter, <s 9(2)(h), that we could use to respond if/when we get media queries on the lost USB.

There is also the question of whether we wait until we get queries or front foot it and put this out as a media release. There are reasons for going proactive which I can outline at this afternoon's meeting.

In the meantime, here is the draft response for you to look at.

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that the information on it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

If any member of the public finds this USB or already has it in their possession Inland Revenue - no questions asked.
Best way to do that??????

Regards,

Gay.

From: Gay Cavill

Sent: Thursday, 28 April 2022 1:59 pm

To: s 9(2)(h) i)

Cc: Rowan McArthur <s 9(2)(a)

<s 9(2)(a) Dawn Swan <s 9(2)(a)

Josh Green

Subject: RE: USB incident - notification

s 9(2)(h) I will distribute them to the meeting members ahead of the meeting.

There is also another decision to be made – do we wait until we get queries or do we front foot it, put it out as a media release and control the release of the narrative. That has the added bonus of us being open, transparent and showing we realise this is not good.

Reactive media response on the loss of the USB of evidence

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information contained in a USB stick and the possibility that the information on it could be accessed by an unauthorised person.

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The USB contains copies of information relating to a criminal prosecution which is currently before the courts.

The USB was being taken from the Freyberg building to Inland Revenue's Upper Hutt Processing Centre for the files to be burnt on a CD-Rom for use in court. When our staff member arrived at the Upper Hutt building, they couldn't find the USB.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. The word 'password' was not written on the note, but anyone who found it could work out that's what it was.

Inland Revenue has searched the staff member's car, retraced the short journey from the Freyberg building to the car, and the Freyberg building itself has been searched.

We are reviewing our processes in relation to this incident. It has been reported to the Police and the Privacy Commissioner has been notified.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual. At this stage, we have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

If any member of the public finds this USB or already has it in their possession Inland Revenue - no questions asked.

Best way to do that?????



From: Dawn Swan <s 9(2)(a)>
Sent: Thursday, 28 April 2022 11:22 am
To: Karen Whitiskie <s 9(2)(a)> Vanessa Johnson <s 9(2)(a)> Joanne Petrie <s 9(2)(a)> Gay Cavill <s 9(2)(a)> Josh Green <s 9(2)(a)> Conrad Bace <s 9(2)(a)>
Subject: USB incident - notification

Hi all

We have decided to notify the individuals affected by this incident and so I attach a draft letter that contains the detail expected in this type of notification.

The third page is a draft notification to the two Corrections staff also.

We will have to do a separate letter for the defendant as we may want to include further information. Karen do you want to manage the content for that letter?

We can discuss later this afternoon.

Dawn Swan
Privacy Officer | Enterprise Design & Integrity | Inland Revenue
Asteron Centre, 55 Featherston Street, Wellington
PO Box 2198, Wellington 6140

 [Call/chat with me in Teams](#) or 021 262 0543

From: s 9(2)(a)
Sent: Monday, 2 May 2022 1:44 pm
To: Karen Whitiskie
Subject: RE: Missing USB - Addresses
Attachments: richarst_1-03-2022_15-18-29.pdf

Hi Karen,

We should probably use the address on his letterhead (see attached):

s 18(c)(i)

From: Karen Whitiskie
Sent: Monday, 2 May 2022 1:36 pm
To: s 9(2)(a)
Subject: RE: Missing USB - Addresses

Hi s 9(2)(a)

The address for s 18(c)(i)

Thanks

Karen

From: s 9(2)(a)
Sent: Monday, 2 May 2022 12:27 PM
To: Karen Whitiskie <s 9(2)(a)>
Subject: RE: Missing USB - Addresses

Looking deeper I did have the address for both of them. I have just sent you this, might still pay to courier them.

Sorry, I'm not sure if its Ms or Mrs

s 9(2)(a)

From: Karen Whitiskie <s 9(2)(a)>
Sent: Monday, 2 May 2022 12:20 pm
To: Andrew Instone <Andrew.Instone@ird.govt.nz>
Subject: RE: Missing USB - Addresses

Also do you happy to know if it is [REDACTED]

Don't search START on this – it is just if you know.

From: s 9(2)(a)
Sent: Monday, 2 May 2022 12:07 PM
To: Karen Whitiskie <s 9(2)(a)>
Subject: RE: Missing USB - Addresses

Hi Karen,

Do you mean the two Officers that were named on the 'sticky' that was on the missing USB?

I only have their email and phone numbers:

s 18(c)(i)

[REDACTED]

Do you want their personal addresses? I would need to contact them or look them up in START.

Regards,

s 9(2)(a)

[REDACTED]

From: Karen Whitiskie <s 9(2)(a)>
Sent: Monday, 2 May 2022 11:26 am
To: s 9(2)(a)
Subject: RE: Missing USB - Addresses

Hi

Can you also give me the details of the two Correction officers and the address to send letters to them?

Thanks
Karen

From: s 9(2)(a)
Sent: Monday, 2 May 2022 9:43 AM
To: Karen Whitiskie <s 9(2)(a)>
Subject: Missing USB - Addresses

Hi Karen,


These are the relevant addresses

s 18(c)(i)



Regards,


s 9(2)(a)



From: s 9(2)(a)
Sent: Monday, 2 May 2022 12:21 pm
To: Karen Whitiskie
Subject: RE: Missing USB - Addresses

That should be fine

s 18(c)(i)



From: Karen Whitiskie
Sent: Monday, 2 May 2022 12:17 pm
To: s 9(2)(a)
Subject: RE: Missing USB - Addresses

Hi

Would we be able to send it to them by courier, care of the prison?

Karen


From: s 9(2)(a)
Sent: Monday, 2 May 2022 12:07 PM
To: Karen Whitiskie <s 9(2)(a)>
Subject: RE: Missing USB - Addresses

Hi Karen,

Do you mean the two Officers that were named on the 'sticky' that was on the missing USB?

I only have their email and phone numbers:

s 18(c)(i)




s 18(c)(i)



Do you want their personal addresses? I would need to contact them or look them up in START.

Regards,

s 9(2)(a)



From: Karen Whitiskie <s 9(2)(a)>
Sent: Monday, 2 May 2022 11:26 am
To: s 9(2)(a)
Subject: RE: Missing USB - Addresses

Hi

Can you also give me the details of the two Correction officers and the address to send letters to them?


Thanks
Karen

From: s 9(2)(a)
Sent: Monday, 2 May 2022 9:43 AM
To: Karen Whitiskie <s 9(2)(a)>
Subject: Missing USB - Addresses

Hi Karen,

These are the relevant addresses

s 18(c)(i)



Regards,

s 9(2)(a)



Legal Services
Inland Revenue
Po Box 2198
Wellington 6140

2 May 2022

s 18(c)(i)

Dear s 18(c)(i)

Inland Revenue takes privacy and confidentiality seriously. As a precautionary measure, we are writing to let you know about a data security incident that involves your personal information. You do not have to take any action.

The incident

On 12 April 2022 a single USB stick was lost on or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The incident was reported internally on 13 April and a meeting was held with the staff member to obtain further information on 14 April.

A Post-It note attached to the USB contained your name and phone number as the staff member was visiting s 18(c)(i) Prison. The USB itself contained no information about you.

The USB was within its packaging, tucked inside a folder. An Inland Revenue staff member carried the folder from their desk in the Freyberg Building to their car which was parked across the road from the building. When the staff member arrived at their destination they could not locate the USB.

Despite a comprehensive search for the USB, to date it has not been located and Inland Revenue has no evidence that it is in the possession of any individual.

The incident has been reported to the Police and the Privacy Commissioner has been notified.

Inland Revenue values your privacy and deeply regrets that this incident occurred. We are reviewing our processes in relation to this incident and will notify you if there are any significant developments.

You have the right to make a complaint to the Privacy Commissioner about this incident. There is information on how to do this on the Privacy Commissioner's website www.privacy.org.nz.

For assistance or to discuss this further, please feel free to contact me. I can be contacted at s 9(2)(a) or the above address.

Your sincerely

s 9(2)(a)

Karen Whitiskie
Legal Services Leader
Inland Revenue



Inland Revenue
Te Tari Taake

Legal Services
Inland Revenue
Po Box 2198
Wellington 6140

2 May 2022

s 18(c)(i)

Dear s 18(c)(i)

Inland Revenue takes privacy and confidentiality seriously. As a precautionary measure, we are writing to let you know about a data security incident that involves your personal information. You do not have to take any action.

The incident

On 12 April 2022 a single USB stick was lost in or around Inland Revenue's Freyberg Building in Aitken Street, Wellington.

The incident was reported internally on 13 April and a meeting was held with the staff member to obtain further information on 14 April.

The contents of the USB were several audio files of interviews relating to the criminal prosecution of s 18(c)(i) s 18(c)(i)

The USB had been prepared as part of Inland Revenue's process for meeting its disclosure obligations in relation to the criminal prosecution. The prosecution case is currently before the s 18(c)(i). Your interview with Inland Revenue is one of the audio files on the USB.

The files on the USB were being transferred to Inland Revenue's Upper Hutt Processing Centre to be burnt on a CD-Rom to enable the files to be provided to s 18(c)(i) as part of meeting the criminal disclosure obligations.

The USB was inside a folder which was carried from within the Freyberg Building to the staff member's car parked across the road from the building. When the staff member arrived at their destination the USB could not be located.

As per standard procedure, the USB was encrypted but the password was written on a Post-It note that was stuck to the USB packaging. While the word 'password' was not written on the note, the numbers and digits on the note could enable someone to access the USB contents.

Actions taken

When the USB could not be located, both the staff member and other Inland Revenue personnel searched through the car, the route to the car from the Freyberg building were retraced, and the Freyberg Building itself was searched. A message was sent to all Inland Revenue staff based in the Freyberg Building asking if they had found a USB stick to deliver it to the Freyberg Inland Revenue mailroom.

To date, the USB has not been located and Inland Revenue has no evidence that it is in the possession of any individual.

The incident has been reported to the Police and the Privacy Commissioner has been notified.

An application has been made to the court for an order under section 199C of the Criminal Procedure Act 2011 prohibiting the publication of the contents of the USB should it come into the possession of any individual.

Next steps

At this stage, we have no evidence that your information has in fact been accessed by a third party, but we also have no certainty over what has happened to the USB. Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to you for this failure.

Inland Revenue is treating this as a notifiable privacy breach under the Privacy Act 2020 despite the fact that we cannot be certain the information has been accessed.

We do not consider that this loss puts you at risk of serious harm as presumed under the Privacy Act for an incident to be a notifiable breach. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

The delay in informing you of this incident was due to it being reported the day before the Easter public holiday period, and time taken to see if the USB was located in or around the Freyberg Building by staff. The USB could not be located following the taking of those steps and further internal Inland Revenue processes. We are therefore now notifying you of the loss of that data.

Inland Revenue values your privacy and deeply regrets that this incident occurred. We are reviewing our processes in relation to this incident and will notify you if there are any significant developments.

You have the right to make a complaint to the Privacy Commissioner about this incident. There is information on how to do this on the Privacy Commissioner's website www.privacy.org.nz.

For assistance or to discuss this further, please feel free to contact me. I can be contacted at s 9(2)(a) or the above address.

Your sincerely

s 9(2)(a)

Karen Whitiskie
Legal Services Leader
Inland Revenue

From: [Eteline Tiraa](#)
To: [Legal Services - Wider Leadership Team](#)
Subject: CONFIDENTIAL: USB process review
Date: Friday, 6 May 2022 12:52:56 pm

Hi,

Some of you or your people may have seen media articles published re the loss of evidence like the one posted on stuff:

<https://www.stuff.co.nz/national/crime/128562101/inland-revenue-loses-evidence-in-fraud-from-prison-case-leading-to-suppressions>

Although this rarely happens, we do need to ensure that our process and policy around ensuring careful management and transporting our information is well understood by our people and is kept secure. Over the next week I will update our USB internal process for you to share with your teams. Although this will be iterative subject to any updates that is made on IR's overall policy and approach on this, we will also look to include this as part of the BMC checks.

I wanted to give you a heads up on this and what needs to be done at pace on this issue. Due to the sensitivity of this issue I ask you keep this confidential and manage any queries that your teams may have on this.

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: [Valerie Johnson](#)
To: [Karen Whitiskie](#)
Subject: Stuff news...
Date: Friday, 6 May 2022 11:57:49 am
Importance: High

[UNCLASSIFIED]

Hi Karen

Not sure if you have seen this...

<https://www.stuff.co.nz/national/crime/128562101/inland-revenue-loses-evidence-in-fraud-from-prison-case-leading-to-suppressions>

Val.

Ngā mihi

Val Johnson | PA/Business Support - Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'
Auckland (Manukau) | New Zealand

s 9(2)(a)





From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: RE: USB process review
Date: Friday, 6 May 2022 12:47:10 pm

Noted – will send it now

From: Karen Whitiskie
Sent: Friday, 6 May 2022 12:42 PM
To: Eteline Tiraa
Subject: RE: USB process review

I am waiting to hear about internal comms. I am happy for a confidential heads up to the wider leadership team but I don't want to get ahead of any wider comms.

From: Eteline Tiraa s 9(2)(a)
Sent: Friday, 6 May 2022 12:34 PM
To: Karen Whitiskie s 9(2)(a)
Subject: USB process review

For matter of transparency I thought I'd send the below out to the wider leadership team – thoughts?

Hi,

Some of you or your people may have seen the stuff article re the loss of evidence:

<https://www.stuff.co.nz/national/crime/128562101/inland-revenue-loses-evidence-in-fraud-from-prison-case-leading-to-suppressions>

Although this rarely happens, we do need to ensure that our process and policy around ensuring careful management and transporting our information is well understood by our people and is kept secure. Over the next week I will update our USB internal process for you to share with your teams. This will be iterative subject to any updates that is made on IR's overall policy on this.

Happy Friday!

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services '*Ratonga Ture*' | Inland Revenue '*Te Tari Taake*'

s 9(2)(a)

From: [Vanessa Johnson](#)
To: [Karen Whitiskie](#)
Subject: RE: USB incident - notification
Date: Friday, 6 May 2022 3:10:02 pm
Attachments: [image001.png](#)
[image002.png](#)

Bother

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue

T. s 9(2)(a)

E. s 9(2)(a)

From: Karen Whitiskie
Sent: Friday, 6 May 2022 12:18 PM
To: Rowan McArthur ; Gay Cavill ; Vanessa Johnson ; Cath Atkins ; Dawn Swan ; Conrad Bace ; Josh Green ; Joanne Petrie
Cc: Kirsty Gemmill ; Jay Harris
Subject: RE: USB incident - notification

Hi

I am following up on how quickly we can get a copy of the order to see precisely what it says.
Karen

From: Rowan McArthur <s 9(2)(a)>
Sent: Friday, 6 May 2022 12:08 PM
To: Karen Whitiskie <s 9(2)(a)> Gay Cavill <s 9(2)(a)> Vanessa Johnson <s 9(2)(a)> Cath Atkins <s 9(2)(a)> Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green <s 9(2)(a)> Joanne Petrie <s 9(2)(a)>
Cc: Kirsty Gemmill <s 9(2)(a)> Jay Harris <s 9(2)(a)>
Subject: RE: USB incident - notification

Gay is now going to do a bit of an NB email to the usual Heads up email list.

Cheers

R

From: Rowan McArthur
Sent: Friday, 6 May 2022 12:06 pm
To: Karen Whitiskie <s 9(2)(a)> Gay Cavill <s 9(2)(a)> Vanessa Johnson <s 9(2)(a)> Cath Atkins <s 9(2)(a)> Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green <s 9(2)(a)> Joanne Petrie <s 9(2)(a)>
Cc: Kirsty Gemmill <s 9(2)(a)> Jay Harris <s 9(2)(a)>
Subject: RE: USB incident - notification

Too late for a heads up then... thanks Karen

From: Karen Whitiskie <s 9(2)(a)>
Sent: Friday, 6 May 2022 12:00 pm
To: Gay Cavill <s 9(2)(a)> Vanessa Johnson <s 9(2)(a)> Cath

Atkins <s 9(2)(a)> Dawn Swan <s 9(2)(a)> Conrad Bace
<s 9(2)(a)> Josh Green <s 9(2)(a)> Joanne Petrie
<s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)> Jay Harris <s 9(2)(a)>
Subject: RE: USB incident - notification

<https://www.stuff.co.nz/national/crime/128562101/inland-revenue-loses-evidence-in-fraud-from-prison-case-leading-to-suppressions>

Hi

See above article.

Karen

From: Gay Cavill <s 9(2)(a)>
Sent: Friday, 6 May 2022 11:51 AM
To: Vanessa Johnson <s 9(2)(a)> Karen Whitiskie
<s 9(2)(a)> Cath Atkins <s 9(2)(a)> Dawn Swan
<s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green
<s 9(2)(a)> Joanne Petrie <s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)> Jay Harris <s 9(2)(a)>
Subject: RE: USB incident - notification

My gut feeling is that we should use the following information from the approved messaging.
s 18(c)(i)

This is not the carefully worded heads up that
Rowan has just messaged about.

Inland Revenue takes privacy and confidentiality seriously. We regret the recent loss of information stored on a USB stick and the possibility that it could be accessed by an unauthorised person.

We are reviewing our processes in relation to this incident. That review is on-going but we anticipate there will be changes as a result of this incident. The loss has been reported to the Police, and the Privacy Commissioner has been notified.

To date, the USB has not been found and Inland Revenue has no evidence that it is in the possession of any individual. We have no evidence that it has been accessed by a third party, but we also have no certainty over what has happened to the USB.

Inland Revenue is disappointed this incident has occurred and would like to sincerely apologise to anyone affected by this privacy breach. We have notified those directly affected. We do not consider that this loss puts anyone at risk of serious harm. However, the USB has been lost and that loss is attributable to Inland Revenue's actions.

Regards,

Gay.

From: Gay Cavill
Sent: Friday, 6 May 2022 11:38 am
To: Vanessa Johnson <s 9(2)(a)> Karen Whitiskie
<s 9(2)(a)> Cath Atkins <s 9(2)(a)> Dawn Swan
<s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green
<s 9(2)(a)> Joanne Petrie <s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill

<s 9(2)(a) Jay Harris <s 9(2)(a)

Subject: RE: USB incident - notification

s 18(c)(i)

From: Vanessa Johnson <s 9(2)(a)

Sent: Friday, 6 May 2022 11:29 am

To: Karen Whitiskie <s 9(2)(a)

Cath Atkins <s 9(2)(a)

Dawn Swan <s 9(2)(a)

Conrad Bace <s 9(2)(a)

Josh Green

<s 9(2)(a)

Gay Cavill <s 9(2)(a)

Joanne Petrie

<s 9(2)(a)

Cc: Rowan McArthur <s 9(2)(a)

Kirsty Gemmill

<s 9(2)(a)

Jay Harris <s 9(2)(a)

Subject: RE: USB incident - notification

We will simply have to wait and see. We have the prepared media messages if needed although it would depend on the question.

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue

T. +s 9(2)(a) |

E. s 9(2)(a)

From: Karen Whitiskie <s 9(2)(a)

Sent: Friday, 6 May 2022 11:24 AM

To: Vanessa Johnson <s 9(2)(a)

Cath Atkins <s 9(2)(a)

Dawn Swan <s 9(2)(a)

Conrad Bace <s 9(2)(a)

Josh Green

<s 9(2)(a)

Gay Cavill <s 9(2)(a)

Joanne Petrie

<s 9(2)(a)

Cc: Rowan McArthur <s 9(2)(a)

Kirsty Gemmill

<s 9(2)(a)

Subject: RE: USB incident - notification

Hi

This just in. s 18(c)(i)

Eight of the eleven letters couriered out have been delivered. There are three where it appears the courier has left a card and not yet delivered. I am monitoring and if not delivered soon we will look at other options.

Two of the eleven have been in touch with me. One of our witnesses who was disappointed about what happened but appreciative of the steps taken. He now has contact from my team around the prosecution to support him as needed. s 18(c)(i)

Ngā mihi

Karen Whitiskie (*she/her*)

Legal Services Leader | Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

T. s 9(2)(a)

E. s 9(2)(a)

From: Vanessa Johnson <s 9(2)(a)

Sent: Monday, 2 May 2022 2:33 PM

To: Karen Whitiskie <s 9(2)(a)> Cath Atkins <s 9(2)(a)>
Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green
<s 9(2)(a)> Gay Cavill <s 9(2)(a)> Joanne Petrie
<s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)>

Subject: RE: USB incident - notification

Looks ok to me Karen

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue

T. s 9(2)(a) |
E. s 9(2)(a)

From: Karen Whitiskie <s 9(2)(a)>
Sent: Monday, 2 May 2022 2:02 PM
To: Vanessa Johnson <s 9(2)(a)> Cath Atkins <s 9(2)(a)>
Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green
<s 9(2)(a)> Gay Cavill <s 9(2)(a)> Joanne Petrie
<s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)>
Subject: RE: USB incident - notification

Hi

Attached is the letter for s 18(c)(i) for any comments.

If I can figure out how to do envelopes, the letters should be ready by the end of the day for the courier.

Thanks

Karen

From: Vanessa Johnson <s 9(2)(a)>
Sent: Monday, 2 May 2022 1:48 PM
To: Cath Atkins <s 9(2)(a)> Karen Whitiskie <s 9(2)(a)>
Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green
<s 9(2)(a)> Gay Cavill <s 9(2)(a)> Joanne Petrie
<s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)>
Subject: RE: USB incident - notification

Good from me

Vanessa Johnson | Service Leader Integrity and Internal Assurance | Whakatūturu pono - Integrity and Internal Assurance | Inland Revenue

T. s 9(2)(a) |
E. s 9(2)(a)

From: Cath Atkins <s 9(2)(a)>
Sent: Monday, 2 May 2022 1:45 PM
To: Karen Whitiskie <s 9(2)(a)> Dawn Swan <s 9(2)(a)>
Conrad Bace <s 9(2)(a)> Josh Green <s 9(2)(a)> Gay Cavill
<s 9(2)(a)> Joanne Petrie <s 9(2)(a)> Vanessa Johnson
<s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)>
Subject: RE: USB incident - notification

Looks good to me.

Noho ora mai

Cath Atkins^(she/her)

Deputy Commissioner Customer & Compliance Services - Business | Inland Revenue Ratonga
Kiritaki Me te Tautukunga - Pakihi | Te Tari Taake
s 9(2)(a) PO Box 2198 | Wellington

From: Karen Whitiskie <s 9(2)(a)>
Sent: Monday, 2 May 2022 1:44 pm
To: Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh
Green <s 9(2)(a)> Gay Cavill <s 9(2)(a)> Joanne Petrie
<s 9(2)(a)> Vanessa Johnson <s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)> Cath Atkins <s 9(2)(a)>
Subject: RE: USB incident - notification

Hi

s 9(2)(h)

s 9(2)(h) Any other comments on the letter content
for the witnesses?

I will shortly send s 18(c)(i) letter.

Thanks

Karen

From: Dawn Swan <s 9(2)(a)>
Sent: Monday, 2 May 2022 1:35 PM
To: Karen Whitiskie <s 9(2)(a)> Conrad Bace <s 9(2)(a)>
Josh Green <s 9(2)(a)> Gay Cavill <s 9(2)(a)> Joanne Petrie
<s 9(2)(a)> Vanessa Johnson <s 9(2)(a)>
Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill
<s 9(2)(a)> Cath Atkins <s 9(2)(a)>
Subject: RE: USB incident - notification

I would keep 10 in there for transparency unless this potentially discloses the number of witnesses involved and
therefore the scope of the case or evidence against the defendant.

The defendant should be told there were 10 files on the USB.

From: Karen Whitiskie <s 9(2)(a)>

Sent: Monday, 2 May 2022 1:21 PM

To: Dawn Swan <s 9(2)(a)> Conrad Bace <s 9(2)(a)> Josh Green <s 9(2)(a)> Gay Cavill <s 9(2)(a)> Joanne Petrie <s 9(2)(a)> Vanessa Johnson <s 9(2)(a)>

Cc: Rowan McArthur <s 9(2)(a)> Kirsty Gemmill <s 9(2)(a)> Cath Atkins <s 9(2)(a)>

Subject: RE: USB incident - notification

Thanks

Attached is the letter to one of the witnesses. All witness letters other than s 18(c)(i) will be the same so I am only going to send one on to you for any comments – unless you want the rest. The only question I had was whether we were leaving the number 10 in or not in relation to the audio files?

Let me know if you have any comments on this.

Thanks

Karen

s 18(c)(i)

Not in scope, Duplicate

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#); [Daniel Hicks](#); [Andrew Tringham](#)
Subject: Fwd: CONFIDENTIAL: USB process review
Date: Friday, 6 May 2022 1:01:16 pm
Attachments: [Information security reminders - PLEASE READ AND NOTE .msg](#)

FYI - I do hope that across all our leads they remember it's privacy week coming up, etc

From: Sanjiv Weerasinghe
Sent: Friday, May 6, 2022 12:55 PM
To: Eteline Tiraa
Subject: RE: CONFIDENTIAL: USB process review

Thanks Eteline.

This will be timely because I sent the attached this morning given that it is privacy week next week. Spooky!

Cheers

Sanjiv

From: Eteline Tiraa
Sent: Friday, 6 May 2022 12:53 PM
To: Legal Services - Wider Leadership Team
Subject: CONFIDENTIAL: USB process review

Hi,

Some of you or your people may have seen media articles published re the loss of evidence like the one posted on stuff:

<https://www.stuff.co.nz/national/crime/128562101/inland-revenue-loses-evidence-in-fraud-from-prison-case-leading-to-suppressions>

Although this rarely happens, we do need to ensure that our process and policy around ensuring careful management and transporting our information is well understood by our people and is kept secure. Over the next week I will update our USB internal process for you to share with your teams. Although this will be iterative subject to any updates that is made on IR's overall policy and approach on this, we will also look to include this as part of the BMC checks.

I wanted to give you a heads up on this and what needs to be done at pace on this issue. Due to the sensitivity of this issue I ask you keep this confidential and manage any queries that your teams may have on this.

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'


s 9(2)(a)

From: s 9(2)(a)
Sent: Friday, 6 May 2022 12:41 pm
To: Karen Whitiskie
Subject: RE: IRD v s 18(c)(i) - case review and suppression

External Email CAUTION: Please take **CARE** when opening any links or attachments.


Hi Karen,

s 9(2)(h), s 18(c)(i)




Ngā mihi | Kind regards

s 9(2)(a)



Level 20, 157 Lambton Quay 6011 • PO Box 10357 Wellington 6143

www.lcc.co.nz



Litigation and public law specialists
Office of the Wellington Crown Solicitor

Please notify us if this communication has been sent to you by mistake. If it has been, client legal privilege is not waived or lost and you are not entitled to use it in any way. While we use standard virus protection software, we accept no responsibility for viruses or anything similar in this email or its attachments, nor do we accept responsibility for changes made to this email or to its attachments after it leaves our system.

From: Karen Whitiskie
Sent: Friday, 6 May 2022 12:20 pm
To: s 9(2)(a)
Subject: RE: IRD v s 18(c)(i) - case review and suppression

[IN CONFIDENCE RELEASE EXTERNAL]

Hi s 9(2)(a)

Do you have a timeframe on the order at all?

Stuff has reported on it so it would be great to have the actual order as soon as possible.

Ngā mihi

Karen Whitiskie (*she/her*)

Legal Services Leader | Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: s 9(2)(a)

Sent: Friday, 6 May 2022 11:09 AM

To: s 9(2)(a)

Cc: s 9(2)(a)

Conrad Bace s 9(2)(a)

; s 9(2)(a)

s 9(2)(a)

Karen Whitiskie s 9(2)(a)

s 9(2)(a)


Crown Prosecutions <cps@lcc.co.nz>

Subject: IRD v s 18(c)(i) - case review and suppression


| |
|---|
| External Email CAUTION: Please take CARE when opening any links or attachments. |
|---|

Hi s 9(2)(a)

s 18(c)(i), s 9(2)(h)




s 18(c)(i), s 9(2)(h)




Ngā mihi | Kind regards

s 9(2)(a)



Level 20, 157 Lambton Quay 6011 • PO Box 10357 Wellington 6143

www.lcc.co.nz



Litigation and public law specialists

Office of the Wellington Crown Solicitor

Please notify us if this communication has been sent to you by mistake. If it has been, client legal privilege is not waived or lost and you are not entitled to use it in any way. While we use standard virus protection software, we accept no responsibility for viruses or anything similar in this email or its attachments, nor do we accept responsibility for changes made to this email or to its attachments after it leaves our system.

This email and any attachment may contain confidential information. If you have received this email or any attachment in error, please delete the email / attachment, and notify the sender. Please do not copy, disclose or use the email, any attachment, or any information contained in them. Consider the environment before deciding to print: avoid printing if you can, or consider printing double-sided. Visit us online at ird.govt.nz

Appendix F

[IN CONFIDENCE]

[illegible]

S
9(2)
(a)

[illegible][illegible][illegible]

s 9(2)(a)

[illegible]

s 9(2)(a)

[illegible]

| s 9(2)(a) | User ID | Group & Requestor Name | Request No | Date Requested | Expiry Date | Expiry Action by SecOps | Exemption Level |
|-----------|---------|------------------------|-------------|----------------|-------------|-------------------------|---|
| | | Anthony McCluskey | RITM0182105 | 17/09/2020 | 18/09/2021 | | The basic exemption to use the USB slots and exemption from having to use Bitlocker |
| | | Anthony McCluskey | RITM0182105 | 17/09/2020 | 18/09/2021 | | The basic exemption to use the USB slots and exemption from having to use Bitlocker |
| | | Anthony McCluskey | RITM0182105 | 17/09/2020 | 18/09/2021 | | The basic exemption to use the USB slots and exemption from having to use Bitlocker |
| | | | | | | | |
| | | | | | | | |

From: Karen Whitiskie
To: Karen Whitiskie
Subject: FW: USB Approved Users Exemption List
Date: Tuesday, 19 April 2022 9:08:45 am
Attachments: Legal- Users with outstanding Security Exemptions Sept 2021.xlsx
image001.png
image002.png

From: Anthony McCluskey
Sent: Tuesday, 21 September 2021 8:24 AM
To: Anthony McCluskey ; Corinna Odlin ; Ele Duncan ; Eteline Tiraa ; Jim Baun ; John Rollo ; Karen Whitiskie ; Maria Szymanik ; Natasha Delamore ; Nathan Wallis ; Raquel Greive ; Rhys Brown ; Rob Falk ; Sanjiv Weerasinghe ; Sarah Shannon ; Shaurya Malaviya ; Tina Moodley ; Tony Munt ; Vaiula Roberts ; Valerie Johnson
Cc: Yolanda Wilke
Subject: USB Approved Users Exemption List

Hi everyone.

We have a bit of house keeping that we need to do in regards to the USB exemption that we have in place for Legal Services. This exemption needs to be renewed every 12 months and allows our staff to use their USB slots and to encrypt USB's to send material out to external parties, our current exemption expires at the end of this month.

Last year I was able to provide a list of everyone within Legal Services, this year however the team that manages this process would like it to be broken down a bit to help manage the process. If each Team Lead submits a request on behalf of the members in their team I think that should work.

The link below will take you to the relevant Support Portal page and I have done an example that you can follow. There isn't a section to add in the names of your team so you'll need to attach them where there is the attachments option at the bottom, just a quick word document listing the team members should be fine.

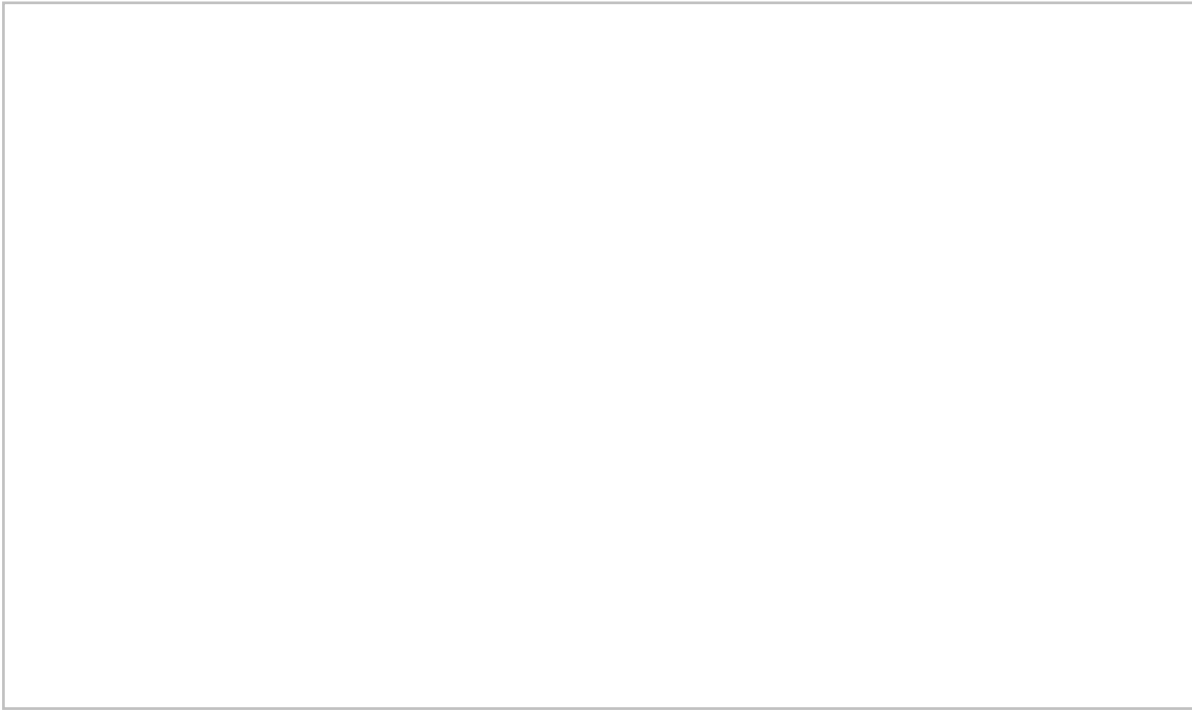
[Support Portal - FSM Service Catalog \(service-now.com\)](#)

The attached excel spreadsheet is a list of those that need to be renewed but in case someone has been missed its probably safer to list out all your team members.

If you have any questions please sing out and I help if I can.

Cheers
Anthony

Not in scope



Anthony McCluskey | Team Lead - Support | Legal Services | Inland Revenue

s 9(2)(a)

From: [Anthony McCluskey](#)
To: [Eteline Tiraa](#)
Subject: RE: USB exemption process
Date: Wednesday, 20 April 2022 11:43:33 am
Attachments: [Legal Services Process for Handling Electronic Storage Device \(ESD\).pdf](#)
[RE Expiry - USB Security Exemption for Legal.msg](#)
[IR Wide Solution for Sharing Information via Cloud.msg](#)
[USB Approved Users Exemption List.msg](#)

The attached PDF is the process we are meant to follow when dealing with USB's.

In regards to the exemption, originally I put through a mass exemption for Legal Services with the addition the BSO's had a full exemption which meant they were not forced to use BitLocker (this was due to the issues we have with BitLocker s 18(c)(i))

The exemptions last 12 months and back in September 2021 we got the heads up to renew (email above re Expiry) I sent out an email to our wider leadership team (email re USB Approved Users...)

I have also included an email I sent to Raquel regarding supplying information to parties. This latest issue again highlights a need for IR to have a better solution than just farming out USB's, maybe the latest drama gets this back on the radar.

Hope this is the kind of information your after, if not happy to have a chat.

Cheers
Ants

From: Eteline Tiraa s 9(2)(a)
Sent: Wednesday, 20 April 2022 11:10 AM
To: Anthony McCluskey s 9(2)(a)
Subject: USB exemption process

Hey Ants – did we do something re getting people to complete and understand the USB exemption process and do we have this documented somewhere that we can pull the report from?

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'
s 9(2)(a)

**LEGAL SERVICES
PROCESS FOR HANDLING ELECTRONIC STORAGE DEVICE (ESD)**

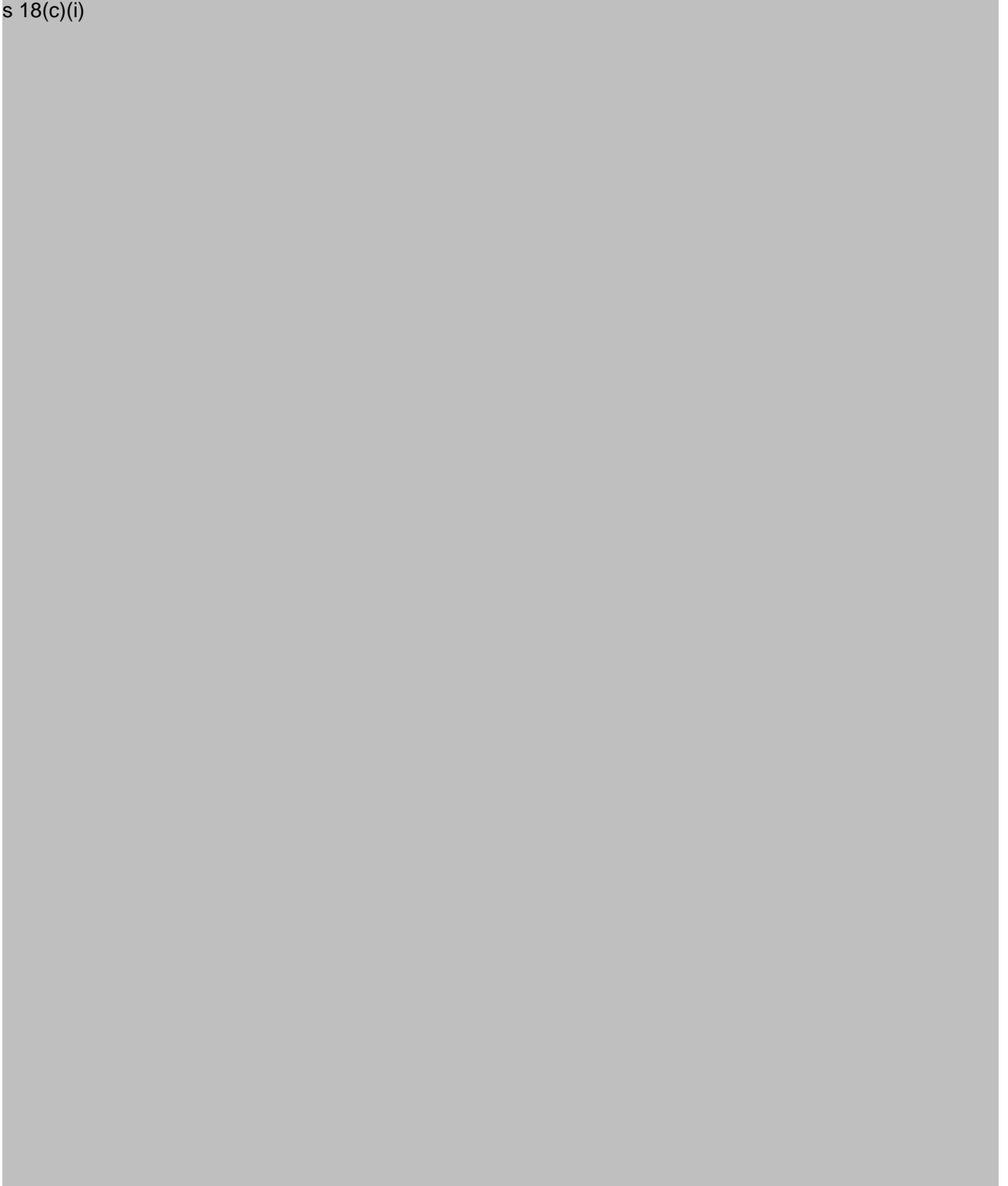
Background

The following process outlines the management of ESD's that are received or sent by Inland Revenue to ensure the integrity of the information is preserved.

A Quarterly reminder will be sent out to all Legal Services and included in the Induction of all new Legal Services staff.

RECEIPT OF DEVICE (IRRESPECTIVE OF SOURCE)

s 18(c)(i)



Solicitors Responsibilities

9. If a LS solicitor requests access of the ESD from the Lock-up room as per paragraph 7 above, it is the LS solicitor's responsibility to keep the EDS secure until it is returned to the Lock up room.(If possible it would be ideal to get the ESD from Solicitor at the end of the day and secure back in the Lock up room.)
- 10.If a LS solicitor receives the ESD directly from a sender, they must give it directly to the BSO assigned to the case. This handover must be recorded on the Case File Index. The file note must provide
 - (a) the date/time the ESD was received by them;
 - (b) the date/time the ESD was provided to the BSO; and
 - (c) the name of the BSO.
- 11.As stated above, this process is to be followed irrespective of the source of the document i.e.: CLO, other external stakeholders or taxpayers.

DELIVERY OF STORAGE DEVICE BY COMMISSIONER TO CROWN LAW AND ANY OTHER PARTY.

s 18(c)(i)



Dated 26 October 2018

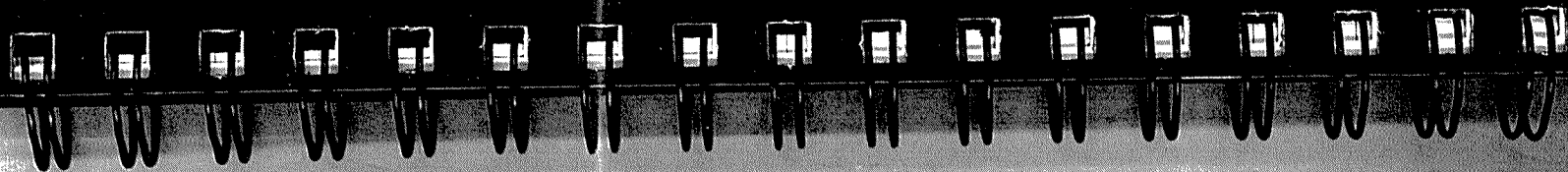
Example of Label to Be used

Crown Law
Level 3, Justice Centre
19 Aitken Street
Wellington 6011

Date
Deliver to:

Description:
Sender Details

U.S. DEPARTMENT OF AGRICULTURE
BUREAU OF PLANT INDUSTRY
WASHINGTON, D. C.



[illegible]

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: FW: PSR Guide - Transporting Documents
Date: Tuesday, 26 April 2022 4:11:34 pm
Attachments: [PSR Guide - Transporting Documents.docx](#)

FYI

From: Ross Walker
Sent: Tuesday, 26 April 2022 4:10 PM
To: Eteline Tiraa
Subject: PSR Guide - Transporting Documents

Hmmm, great question.

Turns out it is not on our site and is out of date.

I have attached it but will need to update it and post it on the site.

Hope this is OK as a guide or I can send you the updated version tomorrow?

Ross

Protective Security Guidelines

Transporting Documents

The following are guidelines for transporting sensitive physical Inland Revenue documents by staff.

Inland Revenue staff have an obligation to take all reasonable steps to maintain the integrity of the tax system and this includes ensuring documents are not released into a public forum in error.

These guidelines are intended to assist staff to make the right decisions when transporting documents.

They are generic, staff should consider the appropriate way to maintain control of the documents based on the circumstances throughout the end to end process of transporting them outside the secure Inland Revenue office environment.

Documents used to support a home visit.

Staff will have documentation containing customers tax information when engaging in home or business premise visits.

- Only take into an address the documents that relate to the customer in the address
- Leave any other documents in the vehicle – store out of sight under a seat or in the boot
- If staff are intending to use public transport or a taxi
 - only take the documentation relating to the customer who is the subject of the visit
 - ensure the documents are in a container with Inland Revenue contact details – some type of envelope or sleeve that contains the documents together

Note: In the event staff may need to exit the premise as a result of a threat the documents are a secondary consideration to staff safety.

Walking Documents Between inner city locations.

Staff carry documents when walking between office locations in an inner city environment.

- Ensure the documents are in a container with Inland Revenue contact details
 - some type of envelope or sleeve that contains the documents together
- Staff should not divert from the intended destination to undertake any other activity such as buying coffee/food etc
- Staff will maintain effective control of the documents throughout the journey

Transporting Documents by Vehicle.

Staff carry large amounts of documents between cities or within a city to specific events such as a court hearing in a vehicle.

- Documents should be stored out of sight preferably in the boot of a vehicle
- Documents should be stored all together or in multiple containers that can be locked
- Staff should maintain contact with the documents at all times
 - If the trip is longer than an hour two staff should accompany the documents
 - If a stop is required one staff member should remain with the documents
 - If a meal break is required is it preferable the documents are secured in an appropriate premise prior to the break
 - If a break is required enroute the vehicle should be parked in a position where staff can see it or one staff member should remain with the vehicle

Transporting Documents by Plane.

Staff carry documents between cities in an aircraft.

- Documents should be in an appropriate locked container such as a suitcase with Inland Revenue contact details attached but not in plain sight
- Where it is practical to do so staff should treat the documents as carryon luggage
- If the documents are checked in staff should ensure they maintain as much contact with them as practicable
 - Be at the collection point prior to the luggage being released into the public space
- Post the flight staff should ensure they maintain control over the documents per transporting between other locations

Related Legislation and Policies.

- Tax Administration Act 1994
- Privacy Act 1993
- Protective Security Requirements (PSR)
- Crimes Act 1961
- Health and Safety in Employment Act 1992
- Powers Manual – Inland Revenue Legal and Technical Standards

Version History

| Date | Document History (Written or Reviewed by) | Name | Next Review Date |
|-------------|---|-------------|-------------------------|
| 20.11.2019 | Written | Ross Walker | Nov 2020 |

From: Eteline Tiraa
To: Anthony McCluskey; Corinna Odlin
Cc: Karen Whitiskie
Subject: FW: USB Approved Users Exemption List
Date: Tuesday, 26 April 2022 4:02:34 pm
Attachments: Legal- Users with outstanding Security Exemptions Sept 2021.xlsx
image001.png
image002.png
RE USB exemption process.msg

Hi Ants,

Thanks again for providing the information on this.

Can I please ask urgently if either you or Corinna can obtain an up to date list on our people with outstanding security exemptions/ yet to complete what they need to do via Service Now and send that through to the leaders to follow up?

From: Anthony McCluskey

Sent: Tuesday, 21 September 2021 8:24 AM

To: Anthony McCluskey; Corinna Odlin; Ele Duncan; Eteline Tiraa; Jim Baun; John Rollo; Karen Whitiskie; Maria Szymanik; Natasha Delamore; Nathan Wallis; Raquel Greive; Rhys Brown; Rob Falk; Sanjiv Weerasinghe; Sarah Shannon; Shaurya Malaviya; Tina Moodley; Tony Munt; Vaiula Roberts; Valerie Johnson

Cc: Yolanda Wilke

Subject: USB Approved Users Exemption List

Hi everyone.

We have a bit of house keeping that we need to do in regards to the USB exemption that we have in place for Legal Services. This exemption needs to be renewed every 12 months and allows our staff to use their USB slots and to encrypt USB's to send material out to external parties, our current exemption expires at the end of this month.

Last year I was able to provide a list of everyone within Legal Services, this year however the team that manages this process would like it to be broken down a bit to help manage the process. If each Team Lead submits a request on behalf of the members in their team I think that should work.

The link below will take you to the relevant Support Portal page and I have done an example that you can follow. There isn't a section to add in the names of your team so you'll need to attach them where there is the attachments option at the bottom, just a quick word document listing the team members should be fine.

[Support Portal - FSM Service Catalog \(service-now.com\)](#)

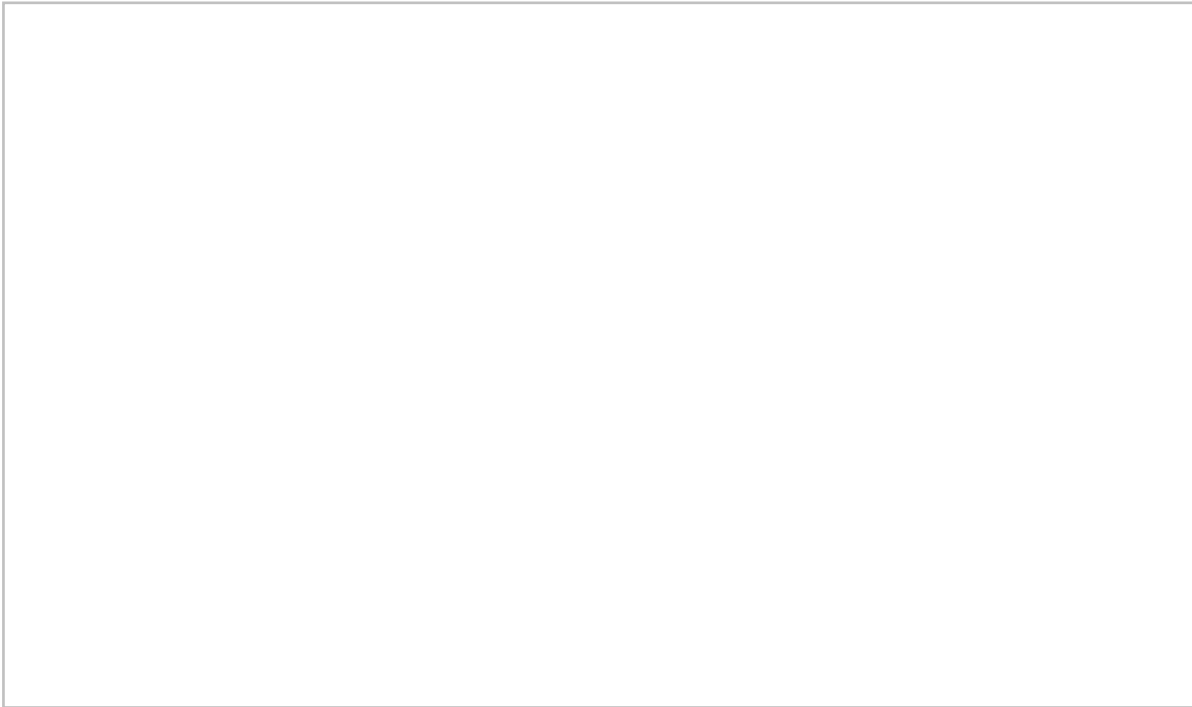
The attached excel spreadsheet is a list of those that need to be renewed but in case someone has been missed its probably safer to list out all your team members.

If you have any questions please sing out and I help if I can.

Cheers

Anthony





Anthony McCluskey | Team Lead - Support | Legal Services | Inland Revenue

s 9(2)(a) [Redacted]

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: Fwd: USB exemption process
Date: Tuesday, 26 April 2022 3:19:02 pm
Attachments: [Legal Services Process for Handling Electronic Storage Device \(ESD\).pdf](#)
[RE Expiry - USB Security Exemption for Legal.msg](#)
[IR Wide Solution for Sharing Information via Cloud.msg](#)
[USB Approved Users Exemption List.msg](#)

This is what I received from Ants on this but clearly shows we need to tighten up the process in this regard

From: Anthony McCluskey
Sent: Wednesday, April 20, 2022 11:43 AM
To: Eteline Tiraa
Subject: RE: USB exemption process

The attached PDF is the process we are meant to follow when dealing with USB's. In regards to the exemption, originally I put through a mass exemption for Legal Services with the addition the BSO's had a full exemption which meant they were not forced to use BitLocker (this was due to the issues we have with BitLocker and MAC devices) The exemptions last 12 months and back in September 2021 we got the heads up to renew (email above re Expiry) I sent out an email to our wider leadership team (email re USB Approved Users...)

I have also included an email I sent to Raquel regarding supplying information to parties. This latest issue again highlights a need for IR to have a better solution than just farming out USB's, maybe the latest drama gets this back on the radar.

Hope this is the kind of information your after, if not happy to have a chat.

Cheers

Ants

From: Eteline Tiraa
Sent: Wednesday, 20 April 2022 11:10 AM
To: Anthony McCluskey
Subject: USB exemption process

Hey Ants – did we do something re getting people to complete and understand the USB exemption process and do we have this documented somewhere that we can pull the report from?

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: Anthony McCluskey
Sent: Friday, 29 April 2022 1:08 pm
To: Eteline Tiraa; Corinna Odlin
Cc: Karen Whitiskie
Subject: RE: USB Approved Users Exemption List

Hi Eteline,

I have requested this information but the main person I deal with is away until 10 May I have included security operations in my request so hopefully we'll get something back.

Cheers
Ants

From: Eteline Tiraa
Sent: Tuesday, 26 April 2022 4:01 PM
To: Anthony McCluskey ; Corinna Odlin
Cc: Karen Whitiskie
Subject: FW: USB Approved Users Exemption List

Hi Ants,

Thanks again for providing the information on this.

Can I please ask urgently if either you or Corinna can obtain an up to date list on our people with outstanding security exemptions/ yet to complete what they need to do via Service Now and send that through to the leaders to follow up?

From: Anthony McCluskey <Anthony.McCluskey@ird.govt.nz>
Sent: Tuesday, 21 September 2021 8:24 AM
To: Anthony McCluskey <Anthony.McCluskey@ird.govt.nz>; Corinna Odlin <Corinna.Odlin@ird.govt.nz>; Ele Duncan <Ele.Duncan@ird.govt.nz>; Eteline Tiraa <Eteline.Tiraa@ird.govt.nz>; Jim Baun <Jim.Baun@ird.govt.nz>; John Rollo <John.Rollo@ird.govt.nz>; Karen Whitiskie <Karen.Whitiskie@ird.govt.nz>; Maria Szymanik <Maria.Szymanik@ird.govt.nz>; Natasha Delamore <Natasha.Delamore@ird.govt.nz>; Nathan Wallis <Nathan.Wallis@ird.govt.nz>; Raquel Greive <Raquel.Greive@ird.govt.nz>; Rhys Brown <Rhys.Brown@ird.govt.nz>; Rob Falk <Rob.Falk@ird.govt.nz>; Sanjiv Weerasinghe <Sanjiv.Weerasinghe@ird.govt.nz>; Sarah Shannon <Sarah.Shannon@ird.govt.nz>; Shaurya Malaviya <Shaurya.Malaviya@ird.govt.nz>; Tina Moodley <Tina.Moodley@ird.govt.nz>; Tony Munt <Tony.Munt@ird.govt.nz>; Vaiula Roberts <Vaiula.Roberts@ird.govt.nz>; Valerie Johnson <Valerie.Johnson@ird.govt.nz>
Cc: Yolanda Wilke <Yolanda.Wilke@ird.govt.nz>
Subject: USB Approved Users Exemption List

Hi everyone.

We have a bit of house keeping that we need to do in regards to the USB exemption that we have in place for Legal Services. This exemption needs to be renewed every 12 months and allows our staff to use their USB slots and to encrypt USB's to send material out to external parties, our current exemption expires at the end of this month.

Last year I was able to provide a list of everyone within Legal Services, this year however the team that manages this process would like it to be broken down a bit to help manage the process. If each Team Lead submits a request on behalf of the members in their team I think that should work.

The link below will take you to the relevant Support Portal page and I have done an example that you can follow. There isn't a section to add in the names of your team so you'll need to attach them where there is the attachments option at the bottom, just a quick word document listing the team members should be fine.

[Support Portal - ESM Service Catalog \(service-now.com\)](https://service-now.com/SupportPortal.do?sysparm_context=ESM%20Service%20Catalog)

The attached excel spreadsheet is a list of those that need to be renewed but in case someone has been missed its probably safer to list out all your team members.

If you have any questions please sing out and I help if I can.

Cheers
Anthony

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: RE: USB
Date: Monday, 2 May 2022 10:00:57 am

Will do

From: Karen Whitiskie
Sent: Monday, 2 May 2022 9:55 AM
To: Eteline Tiraa
Subject: USB

Hi Eteline

Can you make the USB stick review and our processes a priority this week?
I need confidence that everyone is across our processes and that they are being followed. I would also like to know where the storage of the devices are at the moment given the building moves we have had.

Thanks

Karen

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: FW: USB exemption process
Date: Tuesday, 3 May 2022 10:28:52 am
Attachments: [Legal Services Process for Handling Electronic Storage Device \(ESD\).pdf](#)
[RE Expiry - USB Security Exemption for Legal.msg](#)
[IR Wide Solution for Sharing Information via Cloud.msg](#)
[USB Approved Users Exemption List.msg](#)

Lesson learned thus far...

Legal Services process needs to be updated and refreshed. It was last updated in October 2018 although it was sent out as part of a reminder to the team in September 2019 when Anthony was following up on updating the USB Security exemption for Legal Services that needed to be done via the Support Portal and list that IT manage. This process was managed in bulk by Anthony but the issue with this is that the leads are then not familiar with this process and the attached email from IT to Ants does suggest it should be done by leads closer to the people being included to help with them taking more ownership on this (and I also think upskilling with more familiarity of this process) of which I agree. Leads lose sight when these are centrally manage by one person/ or will rely on Ants for what to do.

The process also needs to be tested for improvement where it can be streamlined and easy for users to follow whilst not losing the integrity of keeping the information secure (the process currently includes both an electronic and hard copy register). The process currently notes the Business Support as key contacts to be notified so they can manage recording and tracking of the device with secure information, follow up with scanning of viruses, saving the information electronically and updating the case file accordingly before storing the USB in a centralised lock up space. It's clear that this process wasn't followed with the recent loss of the USB and Business Support weren't advised when it received. The process itself needs to be updated so that it provides enough guidance on how this information should be treated but also allows for people to follow common sense with this (a more principled based approach and balance of transcribing specific steps as required).

I haven't had a further chat with Anthony in this regard but already in my quick chat with Corinna she could only vaguely remember the hard copy book and was not sure where the electronic spreadsheet is saved or whether this was even being updated. It is most likely most of the Business Support team are not too familiar with this process particularly given the recent turnover of people (and the fact not both leads of business support are clear on what this process is).

Recommendation:

- Process is updated and shared with all Legal Services (including each lead to talk through this with their team) – the process should be streamlined so that both solicitors/business support people understand the protocols of security of information rather than centralising the responsibility to Business Support. Noting some areas of improvements needed in how we manage, record and store USB as an example given the current accommodation challenges.
- Update of this process and register is made available on our intranet via Te Matawai
- A business management control on this is added to ensure leaders are across this on a quarterly basis and check to ensure people have been made aware/reminded of this process and their obligation
 - Check on USB approved users is up to date and people are aware/reminded of the process
- The updated process is included as part of the induction of new people
- Post the above short term improvements to be made we could benefit having an initiative

to look further into improvements on how information can be exchanged to prevent loss of physical devices like the USB e.g. exchanging information via the cloud (applications like DropBox) but this would need a bit more work to understand the security implications and working with IT to understand what is feasible in this regard.

Not a detailed of lessons learnt but I'm mostly confident I won't get much in talking to more people as I assume, if like Corrina, most are not too familiar with the process other than Ants. Let me know if want me to take a lead in working through the next steps to improve this.

From: Anthony McCluskey
Sent: Wednesday, 20 April 2022 11:43 AM
To: Eteline Tiraa
Subject: RE: USB exemption process

The attached PDF is the process we are meant to follow when dealing with USB's. In regards to the exemption, originally I put through a mass exemption for Legal Services with the addition the BSO's had a full exemption which meant they were not forced to use BitLocker (this was due to the issues we have with BitLocker and MAC devices) The exemptions last 12 months and back in September 2021 we got the heads up to renew (email above re Expiry) I sent out an email to our wider leadership team (email re USB Approved Users...)

I have also included an email I sent to Raquel regarding supplying information to parties. This latest issue again highlights a need for IR to have a better solution than just farming out USB's, maybe the latest drama gets this back on the radar.

Hope this is the kind of information your after, if not happy to have a chat.

Cheers
Ants

From: Eteline Tiraa s 9(2)(a)
Sent: Wednesday, 20 April 2022 11:10 AM
To: Anthony McCluskey s 9(2)(a)
Subject: USB exemption process

Hey Ants – did we do something re getting people to complete and understand the USB exemption process and do we have this documented somewhere that we can pull the report from?

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: USB exemption update
Date: Tuesday, 10 May 2022 11:15:33 am

Hi Karen,

With the yearly process to request for exemption to use USB, previously being able to submit a bulk request for all our people, in September last year we were notified of the process being changed by IT for exemptions to be applied either individually or their lead.

After a quick chat with Ants, he notes the below:

- Some leaders didn't request it for those that decided their people didn't need it.
- *Ok from the original email I sent out on 21 September 2021 (which included you so you'll have a copy of that one) I spoke with Rob Falk and Tony Munt both of whom though only a couple of people in their team would need the exemptions (those with a litigation background that moved into their teams). Vaiula Roberts and Sarah Shannon also got back to me say they were on to it. Tina Moodley also dealt with it but a few issues which we followed up and dealt with. Jim Baun also dealt with it. Those are the only replies I got. That's not to say others didn't deal with it they just didn't reply.*

The assumption in **s 9(2)(a)** case is that either he requested it himself or it may have been done by his lead otherwise he wouldn't have been able to use the USB on his device. However, this is the theory and reason for requesting the exemption but won't know for sure until we get the updated report from IT which Ants has heard back that it will take a couple of days to generate – expected later this week.

This exemption is for general USB access (using Bit Locker) and only Business Support have full exemption including the use of Iron Keys.

Does this satisfy what you needed to finalise the report on this?

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

From: Eteline Tiraa
Sent: Thursday, 12 May 2022 10:45 am
To: Legal Services - ALL
Subject: FW: Expired USB exemptions

Hi,

Most of you may have received a similar email as listed below to renew your access to have exemption to use USBs on your device.

This should be limited on a needs basis only e.g. court evidence received / created using a USB to exchange information with a third party.

Previously we had most of our people listed to have this exemption which gets renewed yearly.

Other than Business Support who will all continue to require full exemption I would assume that most requests for this exemption would be from those working on litigation.

Thanks,
Eteline

From: Aidan Roberts
Sent: Thursday, 12 May 2022 10:29 AM
Subject: Expired USB exemptions

Hi all,

The Inland revenue information security team (CISO team) has identified that you are currently part of either the partial, or full USB exemption list without a valid record in service now.
You are currently scheduled to be removed from this group on May 20th 2022.

What is required from you:

- If you still require USB access and have a valid business use case please fill out the Service now form "Request a security exemption" available at: [Support Portal - ESM Service Catalog \(service-now.com\)](https://service-now.com)
- If you no longer require USB access you can ignore this email.

Please do not reply to this email.

If you have any concerns please contact s 18(c)(i)

Nga mihi

Aidan Roberts | Information security officer
Enterprise Design and Integrity – CISO Office
Inland Revenue | PO Box 2198 | Wellington 6014



From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: RE: USB process refresh - for your review
Date: Tuesday, 17 May 2022 11:16:08 am
Attachments: [image001.jpg](#)
[image002.jpg](#)

Agreed – I've received minimal feedback but will follow up with the team at the end of the week if I need to get more input.

From: Karen Whitiskie
Sent: Tuesday, 17 May 2022 11:15 AM
To: Eteline Tiraa
Subject: RE: USB process refresh - for your review

I will be interested in the feedback as practically I am not sure this will work given the type of prosecution disclosure going on, the number of Business Support we have and where they are located – and flexible working. My hope is the leaders are talking to their teams on this.

From: Eteline Tiraa s 9(2)(a)
Sent: Tuesday, 17 May 2022 11:12 AM
To: Karen Whitiskie s 9(2)(a)
Subject: RE: USB process refresh - for your review

Yes – to ensure appropriate password protection and encryption – but subject to other thoughts/ feedback on thi

From: Karen Whitiskie s 9(2)(a)
Sent: Tuesday, 17 May 2022 11:09 AM
To: Eteline Tiraa s 9(2)(a)
Subject: RE: USB process refresh - for your review

Hi Eteline

Does this proposed policy mean that only Business Support would transfer material to USB and no solicitors?

Thanks
Karen

From: Eteline Tiraa s 9(2)(a)
Sent: Friday, 13 May 2022 1:20 PM
To: Legal Services - Wider Leadership Team s 18(c)(i)
Subject: USB process refresh - for your review

Hi,

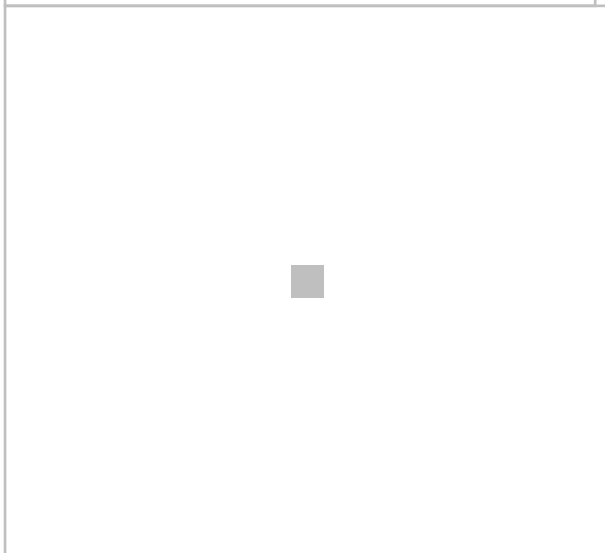
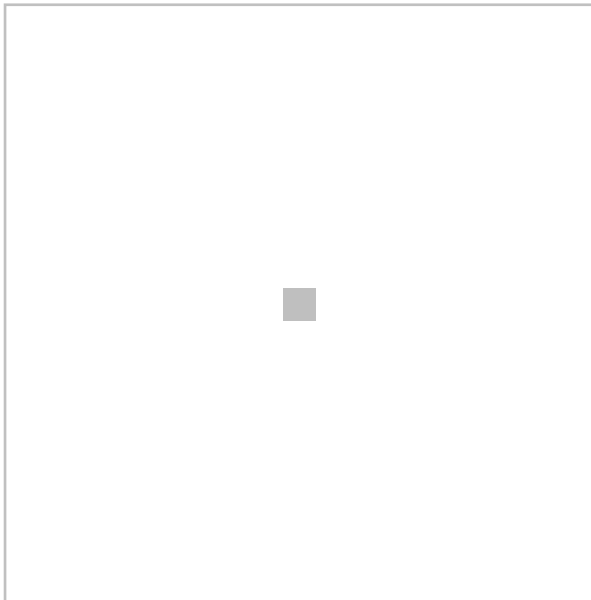
A draft process has been updated and attached for your review. The intention of this refreshed 'USB management of electronic storage device process for Legal Services' will look to replace the previous process also attached. The idea is to keep this simple for our people to follow when required and that it's the responsibility on all our people who receive USBs to manage these carefully and to record appropriately rather than always relying on Business Support to do this.

The exception will be for creating USBs where it makes sense for our Business Support team to do as they will have full USB exemption and can assist with the upload and securely encrypting the USBs we need to upload our information into. I'll also look to include our finalised version on Te Matawai.

A register has also been refreshed as attached and will be saved and linked for the wider team to access.

In terms of actual storage I'm currently thinking of similar options below as the USB will have it's own unique identifier (UID) and to be stored in plastic sleeve below and into a key safe as picture further below. Each site will have a key safe to securely store our USB and the preference will be to keep them in a lock up room that most of our sites will have.

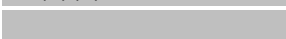
Can you please review this process and send me any thoughts/feedback to finalise this as the interim process for our team (while the wider IR policy is looked at on this). Anthony – can you also send me the steps for how to run a virus scan that we can include with this.



Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)



From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: RE: USB process refresh - for your review
Date: Tuesday, 17 May 2022 11:06:25 am
Attachments: [image001.jpg](#)
[image002.jpg](#)

All good - noted

From: Karen Whitiskie
Sent: Tuesday, 17 May 2022 11:03 AM
To: Eteline Tiraa
Subject: RE: USB process refresh - for your review

Hi Eteline
Just FYI but Cath would like to see our final policy once this is done.
Thanks
Karen

From: Eteline Tiraa <s 9(2)(a)>
Sent: Friday, 13 May 2022 1:20 PM
To: Legal Services - Wider Leadership Team s 18(c)(i)
Subject: USB process refresh - for your review

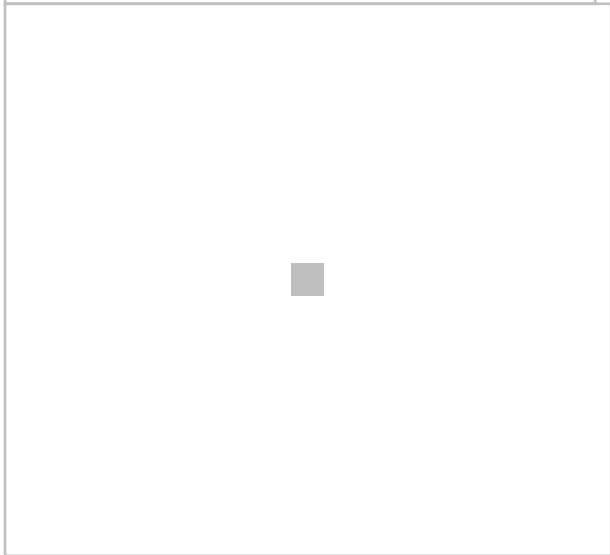
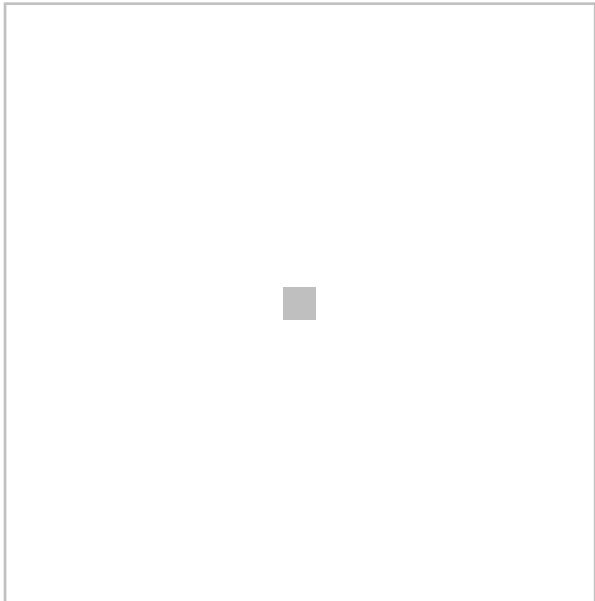
Hi,

A draft process has been updated and attached for your review. The intention of this refreshed 'USB management of electronic storage device process for Legal Services' will look to replace the previous process also attached. The idea is to keep this simple for our people to follow when required and that it's the responsibility on all our people who receive USBs to manage these carefully and to record appropriately rather than always relying on Business Support to do this. The exception will be for creating USBs where it makes sense for our Business Support team to do as they will have full USB exemption and can assist with the upload and securely encrypting the USBs we need to upload our information into. I'll also look to include our finalised version on Te Matawai.

A register has also been refreshed as attached and will be saved and linked for the wider team to access.

In terms of actual storage I'm currently thinking of similar options below as the USB will have it's own unique identifier (UID) and to be stored in plastic sleeve below and into a key safe as picture further below. Each site will have a key safe to securely store our USB and the preference will be to keep them in a lock up room that most of our sites will have.

Can you please review this process and send me any thoughts/feedback to finalise this as the interim process for our team (while the wider IR policy is looked at on this). Anthony – can you also send me the steps for how to run a virus scan that we can include with this.



Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services '*Ratonga Ture*' | Inland Revenue '*Te Tari Taake*'

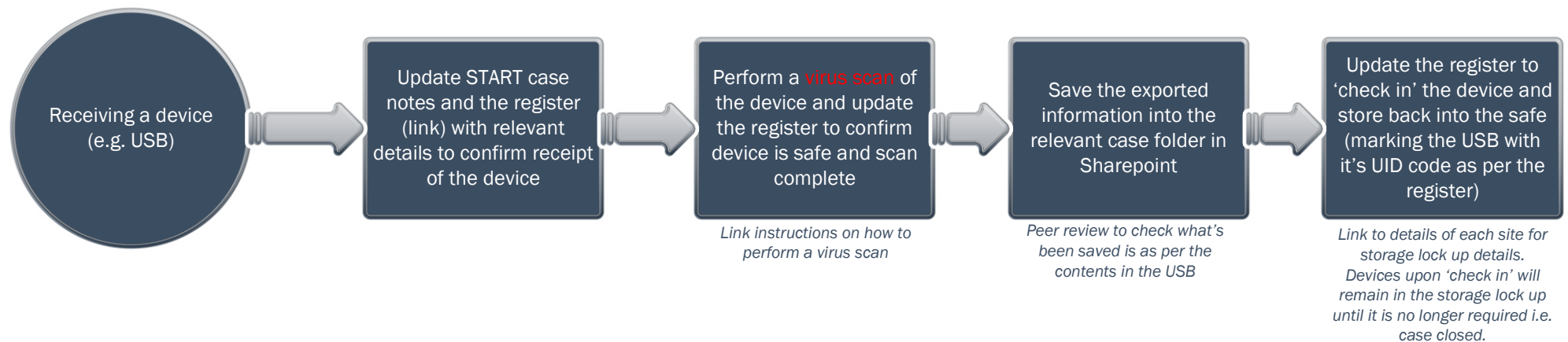
s 9(2)(a)



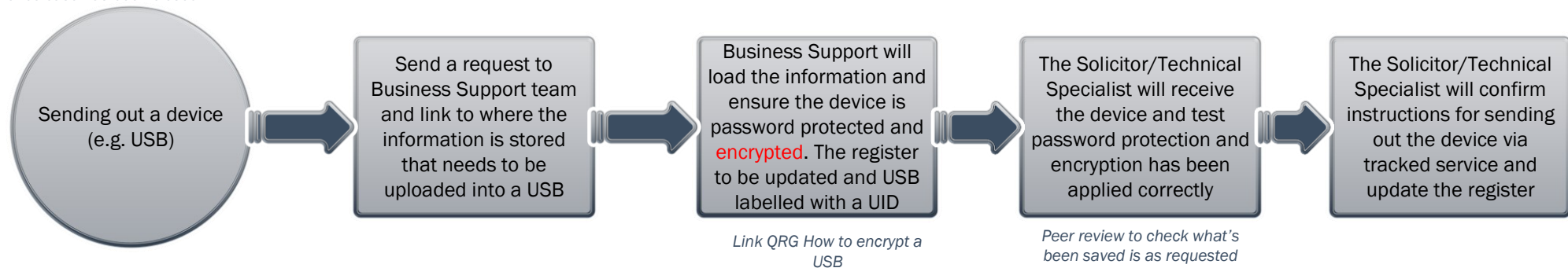
HANDLING OF ELECTRONIC STORAGE DEVICE (ESD) PROCESS

LEGAL SERVICES | updated 16.06.2022

This process outlines how we manage the electronic storage devices that we receive or send out to ensure we preserve the integrity of the information stored in these devices. This mainly covers information we receive or send out with the use of a USB. If we receive or need to send out information electronically by other means please discuss with the Business Support Team Leads to find the best approach on how it should be managed.



At anytime that a USB needs to be accessed out of the safe/ lock up room the register must be updated with 'check out' details and also when being 'check back in'. USB must also be destroyed in the security bin once case has been closed.



- Although some of the steps in this process may be fulfilled by Business Support, the responsibility of ensuring the integrity of the data is maintained is the Solicitor/ Technical Specialist.
- Business Support will manage the purchasing and ensuring appropriate encryption is added on the USB or as appropriate on an Iron Key and apply due diligence on managing the courier of the device whilst ensuring the register is kept up to date.
- Passwords will not be centrally stored to minimise the risk of unintentional / unwarranted access to information. Passwords should be recorded in START.
- The Solicitor/Technical specialist is responsible for storing the password information for their case securely where it is can not be easily accessed / visible for others to access (i.e. a USB should not be marked with labels that include the taxpayer name or password other than the UID as assigned in the register. Passwords should not be sent out together with the USB.
- USB exemption must be applied for via the Support Portal (include link) to request for this exemption when required. This is renewed yearly. All Business Support will request for full exemption to allow them with more options including the need for when an Iron Key or other devices other than a standard USB is required. This process must be shared with people who require the exemption.
- Quarterly BMC framework will include a regular review of this process being shared with their teams along with IR's training on Atea on security and privacy awareness. This is in addition to ongoing discussions each lead need to have regularly with their teams on privacy breaches and regular monitoring of the register and START records in this regard.

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#); [Andrew Tringham](#); [Daniel Hicks](#)
Subject: FW: USB process refresh - for your review
Date: Thursday, 16 June 2022 3:52:56 pm
Attachments: [Legal Services Process for Handling Electronic Storage Device \(ESD\).pdf](#)
[image005.jpg](#)
[image006.jpg](#)
[USB management of electronic storage device process for Legal Services.pdf](#)
[2022.06.16 LS USB register.xlsx](#)

See attached slightly amended from my first draft due based on the feedback I received that I've copied below for your reference. I have also sent a copy of the process and register to Dawn if in case she has any additional feedback. I have not yet heard back from Jay re the wider IR policy to look into this.

In general, limited feedback from Litigation leads, the feedback was in favour of a simple process as outlined. I wonder, as discussed briefly with Andrew, if this can now be passed onto a lead from his group to take ownership of this in socialising and implementing this across the group as well as be the contact to follow up with any ongoing IR policy in this regard given it is primarily his team that deals with USB. This process does however apply to all of LS.

Jim -

Hi Eteline, I only have very general knowledge re this topic and it's not something my team have a regular involvement in but this could change so having a simple, updated process to refer to when the need arises, is really useful/valuable.

Rob -

As it is currently drafted, there seems to be a presumption that ESDs will only be used in Litigation cases. At least that is the way it seems to me as I read it. I don't recall ever receiving information via a USB (or any other ESD) for T/Standards work, but that is not to say that it won't happen. I also assume that Advice may receive USBs from time-to-time. Confidentiality purposes aside, it seems logical that any ESD received on to Legal Services from outside of IR ought to at least be given to a BSO to check for viruses. That being the so, this process ought to apply across all of Legal Services. That point ought to be made explicitly and any references to Solicitor in the process/guidelines ought to be to Solicitor/Technical Specialist.

The guidelines / instructions ought to be clear that although some of the steps may be fulfilled by a BSO, the responsibility for that step still sits with the Solicitor / Technical Specialist.

Where the work is intended to be done by a BSO it would be helpful if that we made clear in the process – perhaps by using different colours for the boxes that the BSO will carry out for the Solicitor / Technical Specialist.

Other than that, the process seems robust. However, rather than relying on the quarterly BMC check either a Team Lead in BS or one of the Tech Leads does some random checks to see that both START and the register are being maintained properly.

Hope this helps.

Ants -

First off looking at the excel spreadsheet it generally looks pretty good and captures what information we should need. The only comments I have are maybe change the 'tab' name to something other than 'Mileage Log', also while I think the one tab is ok, maybe have a tab for incoming and one for outgoing. I know I've discussed passwords with you Eteline so I'd be keen to flesh that out some more I do wonder if we need some place where they are kept, that could well be START but we are relying on people to update that information. I currently have a bunch of USB's that we don't know the passwords for.

In regards to scanning a device for viruses this is a pretty simple task which should involve around 3 steps:

- 1. The device running the scan should be removed from any network connections and effectively be in 'offline' mode, this is in case there are any viruses they don't have a direct path into our system. This would entail making sure the device is not connected to the docking station with a LAN cable plugged in, if the device is using Wi-Fi then it is a matter of turn the Wi-Fi off or putting the device into Flight mode.*
- 2. Once the device is off-line insert the USB. The USB device will appear in your file explore options (often as drive 'D'). Right click the USB device and select 'Scan with Windows Defender' the system will now automatically scan the USB drive*
- 3. If the scan comes back clean you can reconnect to the IR system and upload the material to a location such as SharePoint, if your results come back and show a threat detected then contact the Cyber Security team (don't not reconnect to the network until you have discussed with Cyber Security)*

Just in regards to the above process I am checking in with Cyber Security to make sure it is a process they are happy with and feel that it will met IR's needs, I'll come back to you with any feedback or updated process for that.

In regards to the one pager outlining the process I really like it, nice and simple and doesn't look to overcook the process.

Rhys -

OK so I know very little about USB devices but:

- The end of the first paragraph on the process reads: "in the first instance on best approach in how it should be managed". I think this is just the result of multiple edits but might need to be reworded.
- in relation to "Receiving a device" (top row of the policy), in the last rectangle, we update the register to "check in" the device and store it in the safe. That implies that USBs are re-used. So, do we delete the (incoming) contents at any point, and if so should that be a step in the process? I assume we would want to reduce the risk of leaving files on the USB and sending them out again by accident. But then we also say in the bold type between the two rows that "... USB must also be destroyed in the security bin once case has been closed". Do we keep it for the duration of the case and maybe re-use it for that case if there are multiple exchanges of information, then destroy it? It wasn't clear to me.
- Is there one register for Legal Services as opposed to one per site? If so, should there be something on the register to indicate which site has the USB? Then you can check the register to see how many you would expect to be in the safe for that site (based on check in/check out), and compare it to how many there actually are.
- A USB may have multiple check in/check outs, so it needs multiple lines on the register? Can the spreadsheet be reformatted to make this easier, or at least make it clear for people how this will work (do you insert a new line)?
- Are UIDs re-used for a newly purchased USB? Or does USB LS 001 get used for a case, binned, and that number will never be allocated to another USB? (I'm guessing the latter if "U" is for "unique". But it might be good to clarify).

Katie -

It's actually quite timely because I am expecting a return of USB's from Meredith Connell at some point so it will be good to know the process once I receive them.

Good question – will need to include that they will need to be retrieved and destroyed given we will have saved the electronic information on our database.

From: Eteline Tiraa

Sent: Friday, 13 May 2022 1:20 PM

To: Legal Services - Wider Leadership Team

Subject: USB process refresh - for your review

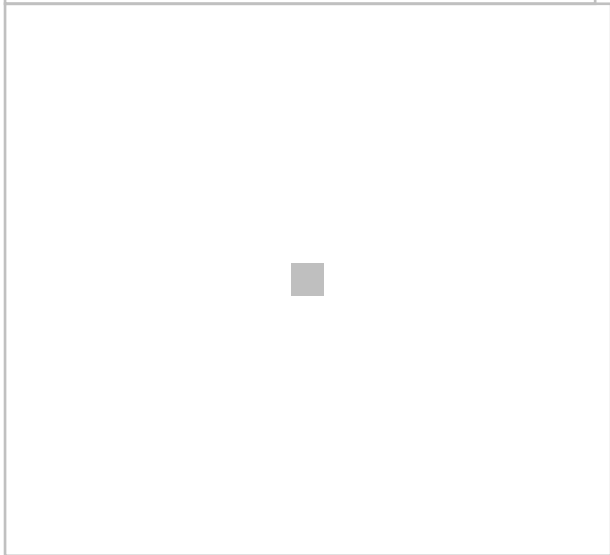
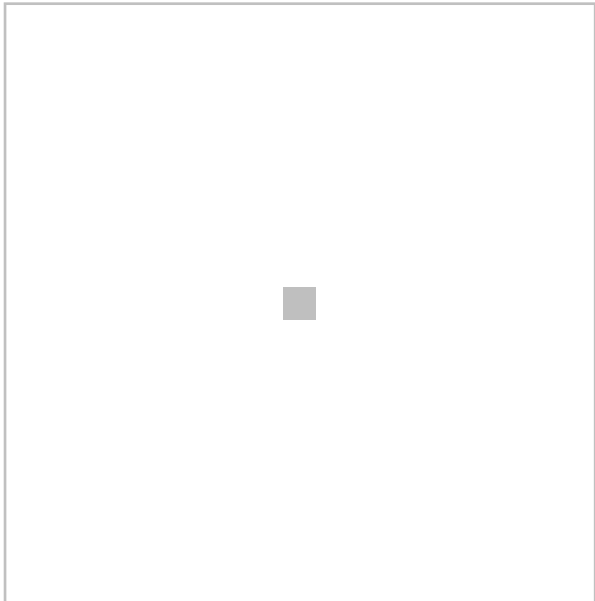
Hi,

A draft process has been updated and attached for your review. The intention of this refreshed 'USB management of electronic storage device process for Legal Services' will look to replace the previous process also attached. The idea is to keep this simple for our people to follow when required and that it's the responsibility on all our people who receive USBs to manage these carefully and to record appropriately rather than always relying on Business Support to do this. The exception will be for creating USBs where it makes sense for our Business Support team to do as they will have full USB exemption and can assist with the upload and securely encrypting the USBs we need to upload our information into. I'll also look to include our finalised version on Te Matawai.

A register has also been refreshed as attached and will be saved and linked for the wider team to access.

In terms of actual storage I'm currently thinking of similar options below as the USB will have it's own unique identifier (UID) and to be stored in plastic sleeve below and into a key safe as picture further below. Each site will have a key safe to securely store our USB and the preference will be to keep them in a lock up room that most of our sites will have.

Can you please review this process and send me any thoughts/feedback to finalise this as the interim process for our team (while the wider IR policy is looked at on this). Anthony – can you also send me the steps for how to run a virus scan that we can include with this.



Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services '*Ratonga Ture*' | Inland Revenue '*Te Tari Taake*'

s 9(2)(a)



From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#)
Subject: FW: USB process review
Date: Thursday, 16 June 2022 2:32:25 pm

Is there someone else specifically looking into this that I can contact as I haven't heard back from Jay on this.

From: Eteline Tiraa
Sent: Friday, 27 May 2022 10:35 AM
To: Jay Harris
Subject: USB process review

Hi Jay,

I understand from Karen that you may looking at reviewing IR's wider policy on managing digital information stored on devices e.g. USB.

We are in the process of finalising our internal process for managing USB devices containing evidence on litigation matters to ensure it's up to date and subject to changes pending the wider IR policy on this.

Is there someone I should test our process on this before we can finalise it for our team?

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

s 9(2)(a)

Note: enter a new row including for a single USB being accessed multiple times

USB Register | Legal Services

[illegible]

| UID (label USB) | Check in Date | USB type (Standard/ IronKey) | Case Name | LS contact | Lock up location | Received From | Sent To | Check out Date | Notes |
|--------------------|------------------|------------------------------------|-----------|------------|------------------|---------------|---------|----------------|-------|
| | | | | | | | | | |
| | | | | | | | | | |

From: [Eteline Tiraa](#)
To: [Karen Whittiskie](#)
Subject: FW: Rosie Tuua shared "BMC 4: System securities" with you.
Date: Monday, 20 June 2022 1:19:05 pm
Attachments: [AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)
[AttachedImage](#)

You happy with this added in our BMC on our updated USB process:

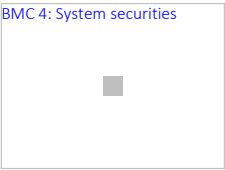
| | |
|--------------|--|
| 4.05 (draft) | (Draft) I can confirm that when my team transfer information on any portable device such as USB external devices, they know and follow Management of electronic storage process for Legal Services |
|--------------|--|

From: Rosie Tuua
Sent: Monday, 20 June 2022 1:14 PM
To: Eteline Tiraa
Subject: Rosie Tuua shared "BMC 4: System securities" with you.

Hi Eteline

Have a look at the draft wording for BMC 4.05 :)

[BMC 4: System securities](#)



[BMC 4: System securities](#)

irnz.sharepoint.com

This control is all about...keeping our information safe. As a people leader, you play a critical role in aligning your people's system access with their roles and responsibilities. My Actions My Evidence 4.01 I can confirm that where a brea...

 [Get the SharePoint Mobile App](#)



From: Eteline Tiraa
To: Karen Whitiskie
Subject: FW: USB process for Legal Services
Date: Wednesday, 24 August 2022 5:31:17 pm
Attachments: USB process for Legal Services draft v0.02.pptx
USB process for Legal Services.docx
image001.png

FYI – I have sent a time tomorrow @11am with Aidan to go through this given his feedback and to help finalise this process. Hopefully not too rude to jump out of our call for this one.

From: Eteline Tiraa
Sent: Wednesday, 24 August 2022 5:26 PM
To: Aidan Roberts
Subject: RE: USB process for Legal Services

Thanks again for your feedback – I've updated both to include your feedback below.
Will set up some time this week to go through this.
Thanks,
Eteline

From: Aidan Roberts s 9(2)(a)
Sent: Friday, 19 August 2022 4:56 PM
To: Eteline Tiraa s 9(2)(a) >
Cc: Craig Scoon s 9(2)(a); Cat Alvarez s 9(2)(a)
Subject: RE: USB process for Legal Services

Hi Eteline,
Thanks for providing this to us, I have spent some time today reviewing and just had a couple of notes to add.
The process overall is good and should provide your staff with some process to align to.

1. Access to USB ports

You will need to add a section in the word document outlining the fact that IR does not allow access for data transfer over the USB ports by default. This is due to the security risk related to information coming into or out of IR. If staff have a need to access information from a USB device they will need to complete a request for USB exemption located in service now at: https://irdnz.service-now.com/esm?id=esm_sc_cat_item&sys_id=34b510ee4f994f007a3998701310c7f6

2. How IR wants to receive information

In the PowerPoint / word doc the wording sounds like staff may often receive information via USB stick, this is really not IR's preferred way to send and receive information and, wherever possible information should be shared via electronic methods. This is due to the risk of inadvertent information disclosure when using USBs.

3. What devices IR uses

IR only permits the use of IronKey USB devices – these are secure encrypted USB devices that are compliant to required security standards. Staff should be made aware in this process that IronKeys **MUST** be used.

If IR has received information from an unknown device this should not be connected to an IR laptop unless absolutely necessary - this should be provided to the IR staff via via electronic method instead

4. The PowerPoint says "passwords will be centrally stored in the register."

Im very unsure about this policy – maybe we need to chat more about how this is being handled – but this sounds like an insecure way to store this – where is this register ?

5. The PowerPoint says "Passwords should not be sent out together with the USB"

This is in fact a MUST requirement. Passwords MUST be sent via a separate channel than the information. Passwords must not be physically provided to the recipient and should be sent electronically instead

6. Around the virus scan:

This sort of implies the device will be untrusted – we want to emphasise that staff should only ever be interacting with Iron Key devices – they should never be trying to use any other sort of usb drive unless there are some odd circumstances.

But again in general the document looks good – definitely a good step forward for the team.

Im happy to meet with you and talk through this feedback etc if you would like let me know

Thanks again

Nga mihi

Aidan Roberts | Information security officer
Enterprise Design and Integrity – CISO Office
Inland Revenue | PO Box 2198 | Wellington 6014

From: Cat Alvarez s 9(2)(a)
Sent: Friday, 19 August 2022 11:15 am
To: Aidan Roberts s 9(2)(a)
Cc: Craig Scoon s 9(2)(a)
Subject: FW: USB process for Legal Services

From: Eteline Tiraa s 9(2)(a)
Sent: Friday, 19 August 2022 11:13 am
To: Jay Harris s 9(2)(a)
Cc: Karen Whitiskie s 9(2)(a); Cat Alvarez s 9(2)(a)
Subject: USB process for Legal Services

Hi Jay,
Apologies for the delay in sending this to your team for review. I had inadvertently thought I had when I sought feedback from others but realised I hadn't in the end.
This is to confirm one of Karen's actions point in finalising this process for our group (can be an evolving document subject to feasible alternative options in place of using USBs is available). I had contacted Cat Alvarez yesterday in your team who has kindly passed this onto another member in your group to review.

The attached process now includes feedback received from:

- Technical Leads and Team Leads – Legal Services
- Dawn Swan, Privacy officer
- Ross Walker, Domain Principal
- Doug Lambert – Enterprise Information and Knowledge

Note a BMC check has also been drafted as part of this process and will be rolled out as a quarterly check that our leads will need to complete subject to the attached being finalised post CISO review of our updated process.

| | |
|--------------|--|
| 4.05 (draft) | (Draft) I can confirm that when my team transfer information on any portable device such as USB external devices, they know and follow Management of electronic storage process for Legal Services |
|--------------|--|

Let me know if you have any further questions on this.

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services '*Ratonga Ture*' | Inland Revenue '*Te Tari Taake*'

s 9(2)(a)

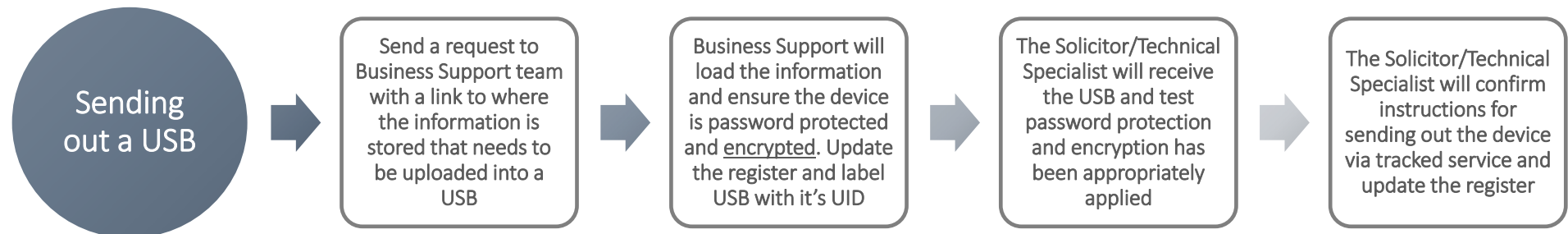
Handling of USB storage device process for Legal Services

Process Owner: Andrew Tringham, Domain Lead | Date updated: 24.08.2022

This process outlines how we manage the electronic storage devices that we receive or send out to ensure we preserve the integrity of the information stored in these devices. This mainly covers information we receive or send out with the use of a USB. Note that the use of a USB is not IR's preferred way to send or receive information. Consideration must first be given wherever possible for the information to be shared via other electronic methods. First discuss the options with the Business Support Team Leads to find the best approach on how it should be managed. If a USB has been received or needs to be sent out the process below must be followed.



At anytime that a USB needs to be accessed out of the safe/ lock up room the register must be updated with 'check out' and 'check in' details. The person removing the device from the safe is the accountable person for the device and must ensure it is in their **control at all times. A USB must also be destroyed in the security bin once case has been closed and it is no longer required.



Notes and useful references

*How to perform a virus scan

1. The device running the scan should be removed from any network connections and effectively be in 'offline' mode, this is in case there are any viruses they don't have a direct path into our system. This would entail making sure the device is not connected to the docking station with a LAN cable plugged in, if the device is using Wi-Fi then it is a matter of turn the Wi-Fi off or putting the device into Flight mode.
2. s 18(c)(i)
3. If the scan comes back clean you can reconnect to the material to a location such as SharePoint, if your results come back and show a threat detected then contact the Cyber Security team (do not reconnect to the network until you have discussed with Cyber Security)

** 'control' means the person knows that it is secure in a locked facility in the office or in an appropriate container when being transported, etc.

Note:

- Although some of the steps in this process may be fulfilled by Business Support, the responsibility of ensuring the integrity of the data is maintained is the Solicitor/ Technical Specialist.
- Business Support will manage the purchasing and ensuring appropriate encryption is added on the USB and apply due diligence on managing the courier of the device whilst ensuring the register is kept up to date.

s 18(c)(i)

- The Solicitor/Technical specialist is responsible for storing the password information for their case securely where it is can not be easily accessed / visible for others to access (i.e. a USB should not be marked with labels that include the taxpayer name or password other than the UID as assigned in the register. Passwords MUST be sent via a separate channel than the information. Passwords must not be physically provided to the recipient and should be sent electronically instead
- USB exemption must be applied for via the Support Portal to request for this exemption when required. This is renewed yearly. All Business Support will request for full exemption to allow them with more options including the need for when an Iron Key or other devices other than a standard USB is required. This process must be shared with people who require the exemption.
- Quarterly BMC framework will include a regular review of this process being shared with their teams along with IR's training on Atea on security and privacy awareness. This is in addition to ongoing discussions each lead need to have regularly with their teams on privacy breaches and regular monitoring of the register and START records in this regard.

Other useful references

[Data, Information, and Knowledge Governance](#)

[Data and Information Policy](#)

[Protective Security – Transporting Documents](#)

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#); [Andrew Tringham](#); [Daniel Hicks](#)
Subject: RE: USB process for Legal Services
Date: Thursday, 25 August 2022 1:26:15 pm
Attachments: [image001.png](#)

Yes he does. If there's an update to the way we currently perform virus scan he was going to send that through.

With the wider IR project looking at how to securely send information electronically underway i.e. via MS 365 I did wonder whether we had anyone / appropriate to have some from LS to provide some input?

From: Karen Whitiskie
Sent: Thursday, 25 August 2022 1:22 PM
To: Eteline Tiraa ; Andrew Tringham ; Daniel Hicks
Subject: RE: USB process for Legal Services

Does Aidan understand USB's will go both ways? Into our team and out of our team?

From: Eteline Tiraa <s 9(2)(a)>
Sent: Thursday, 25 August 2022 11:49 AM
To: Karen Whitiskie <s 9(2)(a)> ; Andrew Tringham <s 9(2)(a)> ; Daniel Hicks <s 9(2)(a)>
Subject: FW: USB process for Legal Services
Latest draft near finalised.

From: Eteline Tiraa
Sent: Thursday, 25 August 2022 11:48 AM
To: Aidan Roberts <s 9(2)(a)>
Subject: RE: USB process for Legal Services
Thanks again for this.
This is the link I have used for USB encryption
[Quick Reference Guide \(sharepoint.com\)](#)

Based on our discussion you happy if I not include the option of Iron Key in this to avoid confusion? Although we do need to work through what appropriate instances would work for the use of Iron Keys that is feasible re cost on some matters.

I've updated both the attached if you have time for a quick review if this is suffice to roll out with our team with a view that this will evolve as required and obviously as new updates are made for alternative solutions, etc.

Thanks,
Eteline

From: Aidan Roberts <s 9(2)(a)>
Sent: Thursday, 25 August 2022 11:30 AM
To: Eteline Tiraa <s 9(2)(a)>
Subject: RE: USB process for Legal Services

Hi Eteline,

Thanks for the meeting today, really appreciate your time.

After discussing today I do understand that its not practical for IR to send data out on IronKeys all times (given the cost and scale we need to operate on)

I also understand that in the future a cloud based secure sharing process would be ideal to remove this dependency on USBs.

I am happy that data can be sent to a persons legal team on a standard USB as long as the following requirements are met:

- All data MUST be encrypted using AES-256 bit encryption (applied via 7 zip software)
- All passwords for the file MUST be generated in line with IRs password policy
 - All character sets (upper case, lower case, number and symbols)
 - Passwords must be 12 characters long
- All passwords MUST be shared via separate medium from the file itself (eg if sent via email password can be sent via sms but NOT via email)

Thanks

Nga mihi

Aidan Roberts | Information security officer
Enterprise Design and Integrity – CISO Office
Inland Revenue | PO Box 2198 | Wellington 6014



From: Eteline Tiraa <s 9(2)(a)>
Sent: Wednesday, 24 August 2022 5:26 pm
To: Aidan Roberts <s 9(2)(a)>
Subject: RE: USB process for Legal Services
Thanks again for your feedback – I've updated both to include your feedback below.
Will set up some time this week to go through this.

Thanks,
Eteline

Not in scope, Duplicate

Handling of electronic storage device process for Legal Services

1 What this Procedure is about

This procedure is for Legal Services regarding the management of the use of information contained on USB devices.

1.1 What business or technical need does this support?

This Process supports the Data and Information Policy and the Protective Security – Transporting Documents

Table of Contents

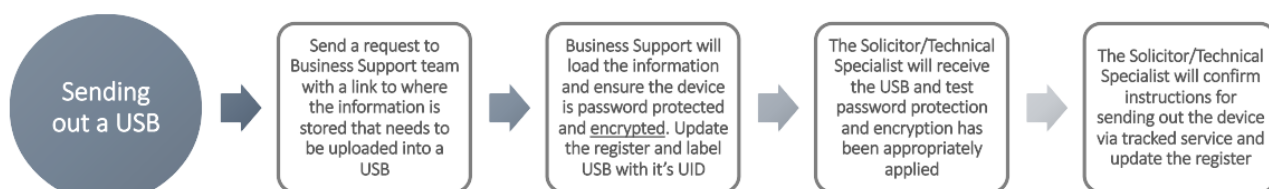
| | | |
|----------|--|----------|
| 1 | What this Procedure is about | 1 |
| 1.1 | What business or technical need does this support? | 1 |
| 2 | What the Procedure is | 1 |
| 3 | Responsibilities | 1 |
| 3.1 | Who does what? | 2 |
| 4 | Terms and Definitions | 3 |
| 5 | Where to find out more | 3 |
| 6 | Document Information | 3 |
| 6.1 | Document amendment history | 3 |
| 7 | Related Documents | 3 |

2 What the Procedure is

This process outlines how we manage the electronic storage devices that we receive or send out to ensure we preserve the integrity of the information stored in these devices. This covers information we receive or send out with the use of a USB. Note that the use of a USB is not IR's preferred way to send or receive information. Consideration must first be given wherever possible for the information to be shared via other electronic methods. First discuss the options with the Business Support Team Leads to find the best approach on how it should be managed. If a USB has been received or need to be sent out the below process must be followed.



At anytime that a USB needs to be accessed out of the safe/ lock up room the register must be updated with 'check out' and 'check in' details. The person removing the device from the safe is the accountable person for the device and must ensure it is in their **control at all times. A USB must also be destroyed in the security bin once case has been closed and it is no longer required.



2.1.1 Access to USB ports

IR (Inland Revenue) does not allow access for data transfer over the USB ports by default. This is due to the security risk related to information coming into or out of IR. If staff have a need to access information from a USB device, they will need to complete a request for USB exemption located in service now at: S 18(c)(i)

2.1.2 What devices IR uses

IR only permits the use of IronKey USB devices – these are secure encrypted USB devices that are compliant to required security standards and **MUST** be used in the first instance if required.

If IR has received information from an unknown device this should not be connected to an IR laptop unless necessary - this should be provided to the IR staff via via electronic method instead if possible.

3 Responsibilities

The following establishes the broad accountabilities and responsibilities of the key internal stakeholders applicable to this Procedure

3.1 Who does what?

| Who | What |
|--|--|
| Leaders of functions, groups, and teams | Technical Leads and Team Leads – to ensure this is included in the induction of new people starting in Legal Services. To complete the quarterly BMC (Business Management Controls) reminder of this process with their teams. |
| All Legal Services employees, contractors, and consultants | Everyone who needs to make use of this Procedure for work purposes should ensure that they understand and comply with this Procedure. |

4 Terms and Definitions

| Term | Definition | Source |
|--|---------------------|-----------------|
| [insert terms alphabetically in table] | [insert definition] | [insert source] |

5 Where to find out more

This Procedure will be available to all employees, contractors, and consultants. The current version of this Procedure is located on IR intranet, Legal Services > [Management of USBs](#). If you require any further information, please contact the Document Owner or Content Developer (refer Section 5.1).

6 Document Information

| | |
|-------------------|--|
| Current version | 18 August 2022 |
| First released | Insert date |
| Last updated | 18 August 2022 |
| Review frequency | 1 year |
| Review Before | 1 October 2023 |
| Business Owner | Andrew Tringham, Domain Lead - Legal Services |
| Document Owner | Eteline Tiraa, Management Support – Legal Services |
| Content Developer | |
| Audience | All Legal Services employees, contractors, and consultants |

6.1 Document amendment history

| Version | Date | Sections amended | Summary of amendment |
|---------------|------|------------------|----------------------|
| [insert text] | | | [insert text] |
| | | | |
| | | | |

7 Related Documents

| | |
|-------|--|
| Title | Data and Information Policy |
| | Protective Security – Transporting Documents |
| | |
| | |

From: [Daniel Hicks](#)
To: [Karen Whitiskie](#); [Eteline Tiraa](#); [Andrew Tringham](#)
Subject: RE: USB process for Legal Services
Date: Friday, 26 August 2022 9:13:13 pm
Attachments: [image001.png](#)

Hi Eteline

This looks good, but I agree that it would make sense (considering the issue we had) to explicitly state in both documents that passwords must be provided separately to the USB.

Cheers

Daniel

From: Karen Whitiskie

Sent: Friday, 26 August 2022 2:43 PM

To: Eteline Tiraa ; Andrew Tringham ; Daniel Hicks

Subject: RE: USB process for Legal Services

Hi Eteline


My only comment is I am still worried about how clear it is that the password should be not be provided with and should be kept separate to the USB?

Andrew/ Daniel – your thoughts?

Thanks

Karen

Not in scope, Duplicate



From: [Eteline Tiraa](#)
To: [Legal Services - ALL](#)
Subject: Updated USB process
Date: Thursday, 1 September 2022 1:38:53 pm

Hi,

We have finalised our USB process and a register to record any USBs we use in our following Sharepoint folder:

[Legal Services - Management of USBs - All Documents \(sharepoint.com\)](#)

A link to this is also on our intranet under Guidelines and Policies:

[Guidelines and policies \(sharepoint.com\)](#)

This process has been updated and reviewed by our leads, IR's Privacy officer, Security Domain Principal, Enterprise Information and Knowledge and CISO team.

Just a reminder that USBs are not an IR preferred device to use and we need to ensure we understand the exemption process for using a USB, ensure proper safe keep of any USB's we use or receive, and confidentially only send out relevant information that is secure and protected in a USB where there is no other option to send the information electronically to external parties. It is important we understand the current risk of using USBs to reduce potential privacy breaches and therefore unwarranted access to IR's information. IR is currently working on an alternative cloud base solution which will ultimately replace the need for USBs.

A BMC check will also be added for each of our leaders to talk you through this process. It will be included in the next quarterly update due in October.

This process is now in effect and the register must be kept up to date to record any existing USBs we have across our sites.

If you have any questions let me know.

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services '*Ratonga Ture*' | Inland Revenue '*Te Tari Taake*'

s 9(2)(a)

From: [Eteline Tiraa](#)
To: [Karen Whitiskie](#); [Andrew Tringham](#)
Subject: FW: USB process
Date: Wednesday, 14 September 2022 4:54:05 pm

I had a meeting with Craig Scoon, from CISO, this afternoon who is now following up on the CISO action points resulting from the lessons learnt USB Incident that Audit are managing.

There are a few suggestions and a project looking at online option of sharing information e.g. via a website that could be a feasible option for us. There may also be a change/control on how we obtain USBs (i.e. control may include requesting these only from a centralised team that has authorisation to purchase these to actively monitor the number / use of them) and to tighten up/reduce risk of potential security breach of information.

Jesse Thwaites and his team are also involved in this project and will be good to have someone from our team in consultation with them to ensure that it will cover what we need as well (look at various scenarios to justify the use of USB vs other alternative options and how the new proposed options could help potential replacing the need for USBs, etc).

I've suggested they contact Anthony and Andrew directly as they progress this work for input when needed.

Hope that works for you Andrew. Officially handing this over....

From: Anthony McCluskey [s 9\(2\)\(a\)](#)
Sent: Wednesday, 14 September 2022 1:19 PM
To: Eteline Tiraa [s 9\(2\)\(a\)](#)
Cc: Andrew Tringham [s 9\(2\)\(a\)](#)
Subject: RE: USB process

Sorry Eteline just now getting to this, yes I'm happy to be included although I might have missed this meeting for today. In any event moving forward happy to be involved.

Cheers

Ants

From: Eteline Tiraa [s 9\(2\)\(a\)](#)
Sent: Tuesday, 13 September 2022 9:54 AM
To: Anthony McCluskey <[s 9\(2\)\(a\)](#)>
Cc: Andrew Tringham [s 9\(2\)\(a\)](#)
Subject: USB process

Hiya – there will no doubt be some follow up on the above including potential import in the wider IR project on the alternative solution that will impact on this process.

I have a meeting tomorrow with Craig Scoon but given I'll be gone for a little bit I wonder if it's worth tagging you into this meeting as well?

Ngā mihi

Eteline Tiraa (she/her) | Management Support, Legal Services 'Ratonga Ture' | Inland Revenue 'Te Tari Taake'

[s 9\(2\)\(a\)](#)

From: [TeamMate@s 18\(c\)\(i\)](#)
To: [Karen Whitiskie](#)
Cc: [Grant Hunt](#)
Subject: TeamCentral Status Update Submission
Date: Friday, 16 September 2022 9:59:19 am
Importance: Low

External Email CAUTION: Please take **CARE** when opening any links or attachments.

A status update has been made by Grant Hunt .

Audit: S0001 : Lessons Learned USB Incident April 2022

Recommendation: 3. Include USB instructions in the Induction Process for all Legal Services staff. [Go to Recommendation](#)

Status Update: We are just incorporating some final comments from the CISO office (Eteline had a follow up discussion with Aiden Roberts yesterday) and will complete all three items at the end of next week.

We will discuss the final version of the policy with our wider leadership team on 1 September after which I will send to the entire team. There have been previous discussions on the draft policy. The BMC check will be included from the next BMC check and it will be included in the Induction Process – we are just trying to figure out the best way to do that.

Confirmation via email that actions have been completed and recommendation can be closed.

K Whitiskie
emails
26 August and 16 September

From: [TeamMate@s 18\(c\)\(i\)](#)
To: [Tony Morris](#)
Cc: [Karen Whitiskie](#); [Grant Hunt](#)
Subject: TeamCentral Status Update Submission
Date: Friday, 16 September 2022 9:07:16 am
Importance: Low

External Email CAUTION: Please take **CARE** when opening any links or attachments.

A status update has been made by Grant Hunt .

Audit: S0001 : Lessons Learned USB Incident April 2022

Recommendation: 16. Review the role/aspect of 'Case Officer' and give consideration around clarifying the role in the new structure [Go to Recommendation](#)

Status Update: I have finalised this by putting into our core documents and training for investigations that it is clear that the CCS Compliance people have ultimate accountability for the course of an investigation from start to finish. This accountability includes ensuring the correct sign-off and real time quality checks are undertaken.

T Morris
16 Sept 2022

From: [TeamMate@s 18\(c\)\(i\)](#)
To: [Karen Whitiskie](#)
Cc: [Grant Hunt](#)
Subject: TeamCentral Status Update Submission
Date: Friday, 16 September 2022 9:57:51 am
Importance: Low

External Email CAUTION: Please take **CARE** when opening any links or attachments.

A status update has been made by Grant Hunt .

Audit: S0001 : Lessons Learned USB Incident April 2022

Recommendation: 1. Review Legal Services instructions for using a USB stick. [Go to Recommendation](#)

Status Update: We are just incorporating some final comments from the CISO office (Eteline had a follow up discussion with Aiden Roberts yesterday) and will complete all three items at the end of next week.

We will discuss the final version of the policy with our wider leadership team on 1 September after which I will send to the entire team. There have been previous discussions on the draft policy. The BMC check will be included from the next BMC check and it will be included in the Induction Process – we are just trying to figure out the best way to do that.

Confirmation via email that actions have been completed and recommendation can be closed.

K Whitiskie
emails
26 August and 16 September

From: [TeamMate@s 18\(c\)\(i\)](#)
To: [Karen Whitiskie](#)
Cc: [Grant Hunt](#)
Subject: TeamCentral Status Update Submission
Date: Friday, 16 September 2022 9:58:38 am
Importance: Low

External Email CAUTION: Please take **CARE** when opening any links or attachments.

A status update has been made by Grant Hunt .

Audit: S0001 : Lessons Learned USB Incident April 2022

Recommendation: 2. Include a check that confirms these instructions are being followed in Business Management Checks. [Go to Recommendation](#)

Status Update: We are just incorporating some final comments from the CISO office (Eteline had a follow up discussion with Aiden Roberts yesterday) and will complete all three items at the end of next week.

We will discuss the final version of the policy with our wider leadership team on 1 September after which I will send to the entire team. There have been previous discussions on the draft policy. The BMC check will be included from the next BMC check and it will be included in the Induction Process – we are just trying to figure out the best way to do that.

Confirmation via email that actions have been completed and recommendation can be closed.

K Whitiskie
emails
26 August and 16 September