MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

30 January 2026

Tēnā koe

Official Information Act request

Thank you for your email of 7 November 2025 requesting a copy of the Ministry of Social Development's (the Ministry's) internal policy, guidance and standard operating produces that governs how staff handle Police requests.

I have considered your request under the Official Information Act 1982 (the Act). Please find my decision on your request set out below.

Please see the attached appendices for the Ministry's internal policy for handling police requests:

- **Appendix One:** NZ Police Requests for Information Training Centralised Services
- **Appendix Two:** Information Sharing CPU Desktop Companion
- **Appendix Three:** Requests for Information (RFIs)
- **Appendix Four:** NZ Police – Warrants to Arrest Request for Information
- **Appendix Five:** NZ Police RFI – Other Common Requests
- **Appendix Six:** Operating protocols for Sharing Information with the Gang Harm Insights Centre
- **Appendix Seven:** Requests for Information from external agencies

Please note that the names and contact details of individuals and certain SEEMail trigger words have been marked and withheld as 'out of scope'.

You will note that the information regarding some individuals is withheld under section 9(2)(a) of the Act in order to protect the privacy of natural persons. The need to protect the privacy of these individuals outweighs any public interest in this information.

Please see the publicly available link to the document on information sharing between the New Zealand Gang Intelligence Centre Agencies which involves the Ministry and New Zealand Police here: https://www.police.govt.nz/sites/default/files/publications/nz-gang-intelligence-centre-approved-info-sharing-agreement.pdf.

I will be publishing this decision letter, with your personal details deleted, on the Ministry's website in due course.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with my decision on your request, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

pp. 

Anna Graham
General Manager
Ministerial and Executive Services

NZ Police RFI - Other Common Requests

This page describes other common requests Centralised Services receives from NZ Police and the process CPOs will follow.

Some Officers may ask for other information. Below is a list of common requests we have seen and the process we should follow when receiving them;

Request reason	**CPO Process and response**
Return of Property	DO NOT provide client details. **Client on current benefit?** Try contacting the client first to advise that we have received information from the NZ Police that they are holding property that belongs to them (be sure to provide them with the Officers name and contact details). **If client contact made – Response to requesting Officer;** *Hi there,* *We are unable to provide you with information based on your reason for request. We have however made contact with the client on your behalf, and provided them with your name and contact details (as per request form). They will contact you to retrieve their property.* *Regards,* **If no contact made or Benefit not current;** Where we are unable to contact the client, or they are not in receipt of a current benefit, we will 1. Add Must View Note to client's CMS record (add 1 year Expiry Date) *If client contact is made, please advise them to contact Police Officer (name) in regards to returning of property.* *Station:* *Contact No:* *Once done, please complete the MVN.* Tip: You can also find the Police station address by clicking on the following link: http://www.police.govt.nz/contact-us/stations [http://www.police.govt.nz/contact-us/stations] 2. Email requesting officer back advising: *We are unable to provide contact details as the reason you require this information does not fall under the exceptions of the Privacy Act.*
Agent's Bank Account	Advise requesting Officer that the client's bank account belongs to their agent and that we are unable to provide this information for this reason.

	If the Officer persists, then they should provide a specified reason for this and explain how this is relevant to their enquiry. If you feel their reason is sufficient, seek manager's approval before providing this information.
Part of a Confidential Investigation	This is not a sufficient reason. Ask the office to clarify the nature of their investigation as we do with all other reasons for requests.
Premises visited	NZ Police may come back to us advising that they have visited the premises of the client and they no longer reside there. Check: **If the client is not in receipt of current assistance;** We will thank the Officer for the information. No further action is required. **If the client is in receipt of current assistance;** 1. Add MVN (Service Delivery > Change in Circumstances > Other) *Information has been received by NZ Police advising they have visited the client's premises (as per address on file) and the client is no longer residing here. As this information has come from an outside agency, we are unable to take further action.* *When client next makes contact, please confirm their correct address and update the system accordingly. If client is in receipt of AS, entitlement may need to be reassessed.*
Partner details	We are not authorised to provide partner details. Response to the requesting Officer: *Hi there,* *Unfortunately we are unable to provide this information as the partner is not the prime suspect. If you require partner information, please send through a new request naming the partner and stating what and why this information is required and how this will help with your investigation.* *Thank you,*
Hard copies of documents (This should only be a last resort as sites do not hold on to hard copies once they have been digitised).	If the Police ask for hard copies of client application forms or documentation, where this is in the client's Scanned Documents then we can provide this information. If we are unable to locate required documents in Scanned Documents, we will; 1. Forward the police request to the Service Centre Manager. 2. Respond to Police advising them that we have forwarded their request for documentation to the Work and Income Service Centre concerned. **Email template when forwarding request to Service Centre Manager** *Hi [SCM name]* *We have received an information request from NZ Police. We are unable to complete this request as it is for documentation which your site holds.*

	Please find attached request for information which the NZ Police have forwarded to us. This request should be considered under the Official Information Act. *Please contact the Police Officer using the contact phone number included in the attached document as soon as possible regarding this matter.* *Thank you and regards,* **Email template when responding to requesting Officer** *Hi [requesting Officer's name]* *Client: [full name and date of birth]* *We are unable to complete your attached request as we do not hold client documentation or files in our office.* *We have forwarded your request to the Work and Income [site area name] Service Centre Manager, [SCM's name] to respond to your request under the Official Information Act.* *We have advised the Manager to contact you directly regarding this matter with the contact number provided on your request.* *Regards,*
Suspend Benefit Request (SBR) OR Statement Request	These two types of requests will be managed by the Mangere team. If you receive an SBR or Statement Request, forward this to: • Out of Scope • Out of Scope • Out of Scope If you are unsure if one of these CPOs are available, send the request to all 3 CPOs or escalate the request to a Mangere Centralised Services Mangere.

NZ Police / Warrants to Arrest Request for Information

This page describes the process that is followed by Centralised Services in response to a request for information from the New Zealand Police.

On this Page:

Introduction

Background

The New Zealand Police request information from Work and Income about a person to enable them to prevent, detect, investigate, prosecute and punish offences.

Legislation

Under the Privacy Act 1993 – Section 6 Principle 11 (e) (i) and (iv) [http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html?search=ts_act_privacy_resel&p=1] , the New Zealand Police have the right to request information deemed necessary in order to maintain the law or conduct court proceedings.

Our Role

Since August 2010 Centralised Services Process Unit has managed this work.

The NZ Police complete an official email template and request personal information regarding people of interest to them and email these requests to us.

Where there are reasonable grounds for requesting client's information, it is our responsibility to search for the requested information in our systems and complete the response.

Response Time

All requests are to be replied to within 24 hours (with the exception of any requests which come through over the weekend or public holidays. These must be responded to by close of the following working day).

The Process

Providing the right information

Under the Privacy Act we are given authority to release any personal information about a client if we believe there are reasonable grounds and it is required in order to maintain the law. However, if the client is deceased, this request will then fall under the Official Information Act.

The information we provide can include but is not limited to person details such as current and previous benefit details.

Where we are not certain why information is required and of what relevance it is to the police, we can contact the Police Officer directly to ask why the information requested is needed, and of what relevance is has to their investigation.

Examples of information not provided unless a necessary reason has been specified include Social Welfare Numbers, agent bank accounts, client's work details and partner details.

Identifiers

In all cases we need to complete an identification check.

The NZ Police must provide us with at least two identifiers in order for us to match their request for information with the client information held in CMS (although we prefer three identifiers).

Where NZ Police have not provided us with sufficient details to make an accurate match in CMS we should email the requesting officer back and request further identifying information e.g. address, date of birth, other known aliases.

Locating the information

Once we have deemed that the information requested meets the standards and at least two identifiers have been provided to locate the client, we will search their information using CMS.

In most cases, NZ Police will provide the client's full name, date of birth and last known address.

Searching for client using payment card details

If NZ Police provide us with the full payment card number, we are able to search for this in CMS to locate client details. Process:

Open CMS and click on 'Workspace tab'

Open up shortcuts and click on 'Advanced Functions' latch

Click on 'Maintain Payment Card'

Add payment card number and click Search

Click here [http://doogle/documents/business-groups/helping-clients/service-delivery/centralised-services/centralised-services-cpu/requests-for-information/client-search-using-payment-card-details-211217.docx] for a breakdown of this process (screenshots included).

NZ Police have only provided partial payment card number?

Put the request on hold in STP (add note stating "Awaiting information from Intel")

Email INTEL unit at Out of Scope (INTEL will assist us in finding the client in CMS as we will not be able to search for client with a partial payment card number)

Advise the Officer that you need to get further information from another business unit before you can provide the information they've requested

Once INTEL has provided us with the information, we will send this to the requesting Officer

Pull up the STP task for this that you put on hold and 'Complete'

Responding to Requests

When responding to requests for information, ensure that you 'Forward' the email so the original Request is attached to your response.

If responding to a request that now falls under the Offical Information Act i.e. deceased client, you must cc: your response to Out of Scope and include in your response, *"As you have advised that this client is deceased, their information no longer falls under the Privacy Act. This information is being released under the Official Information Act."*

Unable to locate the client

If you cannot locate the client you will respond to the requesting Officer stating:

"We were unable to match this person with the information provided.

Please advise if they are known by any other information such as another alias, middle name, past or alternative addresses or a different Date of Birth.

Please include any updates in the request form."

If you are still unable to locate the client with the additional information provided NZ Police, response should be:

"Unable to locate this person with the information provided"

Completed Requests

Once we have completed the request for information, we must ensure that we are 'filing' our requests in the appropriate folder.

Filing the NZ Police requests in the appropriate folders is our electronic form of "batching" for this area of work.

C/O (care of) Address

Where the address is 'C/O' someone, we can provide the address details but we will remove the persons name i.e 'C/O: 123 Babablack sheep Lane'

Emergency Housing (EH) Clients

If you have a reason to believe that the client is currently in Emergency Housing i.e. current benefit but address listed as 'No fixed abode', please check the Hardship Assistance screen and Client Event Notes for any emergency housing details i.e. name of EH, dates booked and the address (if available).

Unverified Address

We will not provide any 'unverified' postal address.

'Unverified' addresses are used for Collections purposes only. There should always be a residential address on file, and this should be used.

Deceased Clients - OIA

If you receive a Police request regarding a deceased client then that request for information will no longer be a Privacy Act request. This is because the Privacy Act provisions do not apply to deceased individuals. The request should be treated as a request for information under the Official Information Act.

You will need to determine if you have any grounds for declining a request for official information here [https://doogle.ssi.govt.nz/map/legislation/guidelines/official-information-act-1982-guidelines/declining-a-request-for-official-information.html] .

You must include the following in your response and CC Out of Scope in:

'As you have advised that this client is deceased, their information no longer falls under the Privacy Act. This information has been released under the Official Information Act.'

If you receive any other requests for Official Information i.e: Government process, please consider sending this section of the request to OIA_Requests@msd.govt.nz if you are unable to locate the information yourself.

Please note that all requests under the Official Information Act must be responded to within 20 working days as a legal requirement.

Further information is available in MAP: Official Information Act 1982 guidelines : Contents - Map (ssi.govt.nz) [https://doogle.ssi.govt.nz/map/legislation/guidelines/official-information-act-1982-guidelines/index.html]

Request for Information Official Template

When NZ Police send requests for information, they must complete a formal template.

In this template the Police should provide the following;

Specifically state "Privacy Act Section 6 Principle 11 (e) (i & iv)

State the name of the person, their date of birth and last known address

Clearly advise what information is required

The reason for the request for information

The name, QID, Station (location) and a contact number of the requesting Officer

If any of the above are not provided, you cannot complete the request. You will respond to the requesting Officer with what is required so they can amend the RFI and return for processing.

Police are able to request information using any of the following templates:

Information Request (IRF) form POL 4135

General Warrant Request (GWR) form POL 4141

Public Safety Information Request (PSIR) form POL 4140

Stop Benefit Request (SBR) form POL 4146

Please note: We do not hold copies of the NZ Police request templates.

Old Request for Information Template received

If you receive the old email template you will forward this back to the requesting Officer using email template below;

"Hi [requesting officer's name]

There have been some changes to how you will request information from Work and Income.

Work and Income along with New Zealand Police have redesigned this process and developed a new request form and an agreement was made that ALL Police requests must come through on these forms. The new template will include [SEEMail] which will keep these requests secure.

If you have any queries or questions regarding the new process, please email or contact your District Prevention Manager.

You will need to resend your request (one request per email) for processing on the new, correct Police Request form.

Thank you and regards,

[your signature inc. SEEMail]"

More than one request as an email attachment

The Police quite often send two or more requests through on one email attachment. The standard process is one request per email.

You will need to forward the email back to the requesting Officer and advise that they should send one request per email - it is easier to process one request at a time and to keep track of the requests.

Reason for Request

Sufficient reasons

The following examples are sufficient to complete the Police Officers request;

Investigation into a burglary

Suspect in theft investigation
Is in Breach of Court Bail and concerns of safety
Client is sought for a burglary that occurred
Required to be located, to be arrested and deal with for cheque fraud
Client has a Warrant to Arrest (WTA) for failing to appear at the District Court
Required to be located and spoken to in relation to two incidents of fraud
For service of a summons to appear in court
Wanted to serve a DNA compulsion notice on
Drugs investigation
Sexual abuse
Domestic violence
Traffic offence

Insufficient reasons

The following examples require further information before a request is completed;

Client is a victim of a serious matter and needs to be located
Wanted/Witness to be interviewed
Criminal investigation
Police file number
Active charges

If you do not feel that the reason the Police are requesting information from us is reasonable e.g. “need to talk to this person”, you should email the Police to seek clarification.

'Confidential' reason

NZP must provide a sufficient reason for requesting information If a request comes through with 'confidential', we must ask the office to clarify the nature of the investigation.

Other reasons

Some Officers may ask for other information. Click here [http://doogle/business-groups/helping-clients/service-delivery/centralised-services/centralised-processing-unit-cpu-/requests-for-information/nz-police-rfi-other-common-requests.html] for other common requests received from NZ Police and the process we should follow.

Types of Information we can provide

If requested, we can provide information including;

Client's name(s)
Date of Birth
Address(es)
Phone number(s)
Benefit details

Other client information

Click here [http://doogle/documents/business-groups/helping-clients/service-delivery/centralised-services/centralised-services-cpu/requests-for-information/locating-client-details-in-cms-221217.docx] for breakdown of where specific client information can be found in CMS (includes screenshots).

Non-current Benefit

Where the NZ Police request information for our clients whose records are non-current (suspended/expired/cancelled/registered/declined/cond grant), we should advise them as such:

Address information requested (non-current benefit)

"Last known address..."

Benefit status requested (non-current benefit)

"This record is not current since [date benefit stopped]"

Address Information

Where our clients have a current postal address which is a street address, we should give both the residential **AND** postal addresses (where they are requesting address information. For example;

Residential address (current from 15/08/15)

s9(2)(a)

Postal address (current from 21/03/15)

s9(2)(a)

The reason we provide this information is that more often than not, the person the Police are enquiring about can be contacted through residents at the postal address; therefore we are trying to provide a better service to the Police.

Postal Addresses (PO Box / Private Bag)

Where our clients have a current postal address which is either a PO Box or Private Bag, we should not give the NZ Police these details. It is no likely that the NZ Police are trying to post a letter to our clients.

Collections Addresses

You will only provide a “Collections address” for clients with an active Collections Case. For all other client’s without an active Collection Case, we will not provide a Collections address.

To check for an active Collections Case, navigate to client’s CMS home page and check below the Actions button.

Click here [http://doogle/documents/business-groups/helping-clients/service-delivery/centralised-services/centralised-services-cpu/requests-for-information/how-to-check-for-an-active-collections-case.docx] to see what this looks like in CMS.

Request for Address Sweep

There are times where the Police ask for the details of “occupants of an address”; this is usually referred to as an ‘Address Sweep’. The ‘sweep’ is completed through a portal and the information is delivered to you the next day via email. To do this, follow the process below;

Open the address sweep tool (link: http://sweb005.corp.ssi.govt.nz/MessageBoard/address_login.asp [http://sweb005.corp.ssi.govt.nz/MessageBoard/address_login.asp])

Enter your username to login

Select the Address Sweep tab

Enter the address details (if the client resides in an apartment or flat, we will only enter the house number). Example; 71A Smith Street - we will provide 71 Smith Street.

IAP will email you the results the following day in a spreadsheet

If the Police Officer has requested other information alongside the address sweep, you should provide a response to this and advise that an Address Sweep is underway and the information will be available within 24 hours.

Receiving the Address Sweep

The response from Intel will be returned to you (the requestor). Ensure you have an email 'rule' set up to identify these requests so they can automatically move to the shared NZP newsgroup.

The information from Intel will be presented on an excel spreadsheet

Providing the Address Sweep information to NZ Police

Once the address sweep is received, we will need to complete the following steps before providing our response;

Open the spreadsheet and filter out the 'current' clients only

Check that the address in the spreadsheet matches the address that was provided on the original request

Where the information is the same, provide client names in a new response to the requesting Officer

Where the information is not the same, advise the requesting Officer: "*We have no record of any other occupants residing at the address provided*"

Where all contact details have been requested, you will need to search for the client in CMS to provide this information (address, phone, call)

Future Appointments

We can provide NZP with any future appointments that may be booked for the client. Their most recent appointment can be viewed on the CMS home page.

All appointments can be viewed via the Appointment Booking Tool (ABT) found in CMS:

Service Delivery Tab

Other Systems latch > Appointments

Booking types:

'Face to Face' - appointment in the office with a CM

Phone - appointment via phone, managed by a CM in the office

Third Party Information

When we receive client information from a third party (e.g., updated contact details), we will create a Must View Note with the following details:

Business Group: Service Delivery

Event Type: Change in Circumstances

Event Sub-Type: Other

Description: Next person to speak with the client, please confirm details

Client event note: CPU has received information from Police: [insert details of the information]. As this information came from an external source, CPU cannot update the client's file directly. Please confirm these details with the client and update the file if necessary

You will need to add an expiry date of three months to your must view note.

Content owner: Work and Income Centralised Processing Unit (CPU) **Last updated:** 20 November 2025

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

NZ Police Requests for Information Training
Centralised Services

Learners Guide

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Session Outline: Day 1

	Introduction – Welcome – Ice Breaker Activity – Session Outline – Learning Objectives & Key Messages – Overview of the day	**20 minutes**
	Overview – Background – Legislation – Our Role – Managing the work	**20mins**
	The Process – Identification process – Providing the right information – Reasons for the request – Unable to locate the client – Non-current benefit – More than one request – Address sweep – Locating the information	**60 mins**
	Systems – Straight to Processing – Filing and how we respond (Outlook) – Ready for Processing Queue process	**10 minutes**
	Practice makes perfect! – Demonstration – Live Actions	**280 minutes**
	Wrap up and close	**10 minutes**

Total timing: 6.5 hours

Introduction

Learning objectives	By the end of this learning, you will be able to: • Demonstrate an understanding of what a Police Request for Information is • Demonstrate an understanding of reasons why the NZ Police request this information, and why we provide it • Show knowledge of how the Police request for information are managed by Centralised Services Processing Unit
Key Messages	• At Work and Income everything we do is about people – helping New Zealanders to help themselves to be safe, strong and independent. • The success of the work that you do relies on your ability to understand what is required of you and be able to transfer your classroom learning into the live environment.

Overview

Today, we will be covering the following:

- Background of NZ Police Requests for Information
- How the work is managed
- The Process
- Demonstrating the Process
- Live Actions

Background

The New Zealand Police request information from Work and Income about a person to enable them to prevent, detect, investigate, prosecute, and punish offences.

Legislation

Under the Privacy Act 1993 – Section 6 Principle 11 (e) (i) and (iv), the New Zealand Police have the right to request information deemed necessary to maintain **the law or conduct court proceedings.**

The full legislation can be found by copying the link below into your browser:

http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html?search=ts_act_privacy_resel&p=1

Our Role

Since August 2010 Centralised Services Process Unit has managed this work.

The NZ Police complete an official email template and request personal information regarding people of interest to them and email these requests to us.

Where there are reasonable grounds, we are responsible for locating the requested information, and completing the response.

Response time – Service Level Agreement (SLA)

All requests are to be replied to within **24 hours** (except for any requests which come through over the weekend or public holidays. These must be responded to by close of the following working day).

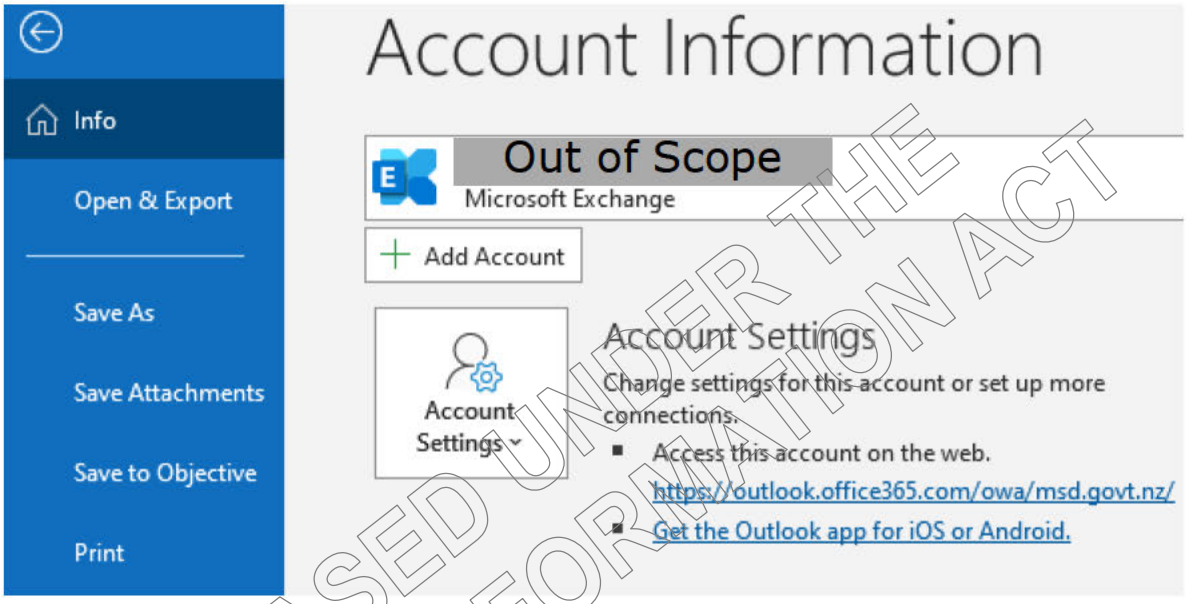
Managing the work

The NZ Police Requests for Information are managed through the Straight to Processing Tool (S2P). Responses are filed in the NZ Police newsgroup (shared email) and should be manually moved from your personal email sent box at the end of each action. We will cover this more as we go through the process.

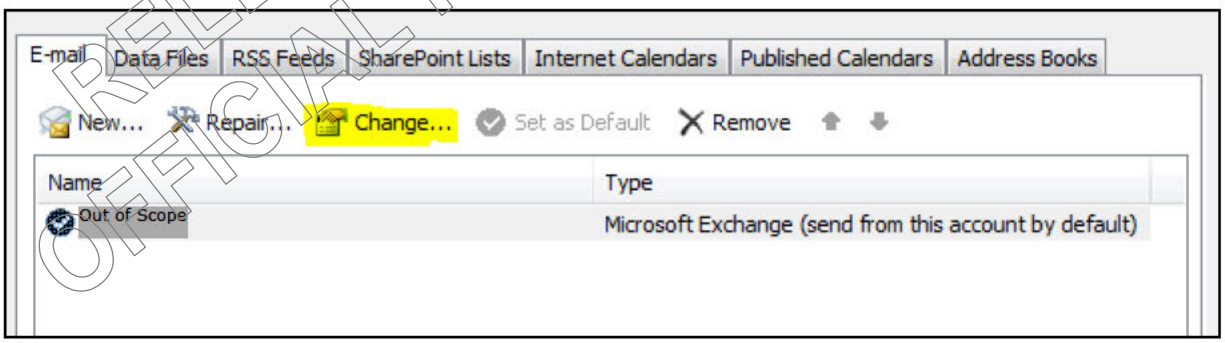
Setting up the newsgroup

By following the steps in your learner's guide, you can set up the NZ Police newsgroup in Outlook. We will do this a bit later - (move to next section)

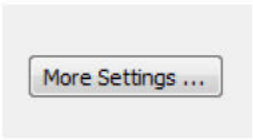
- Through the 'File' tab, locate **Info** and click on:
  - **Account Settings**
    - Account Settings



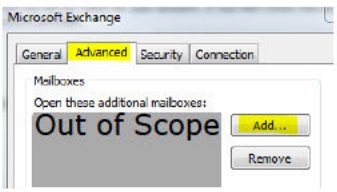
- Click 'Change…'



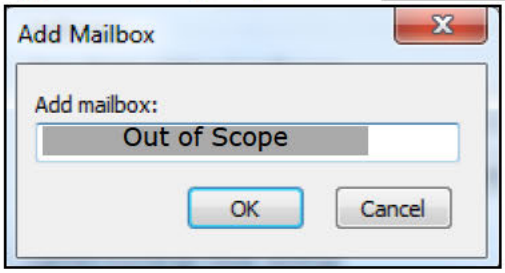
- Click 'More Settings…'……



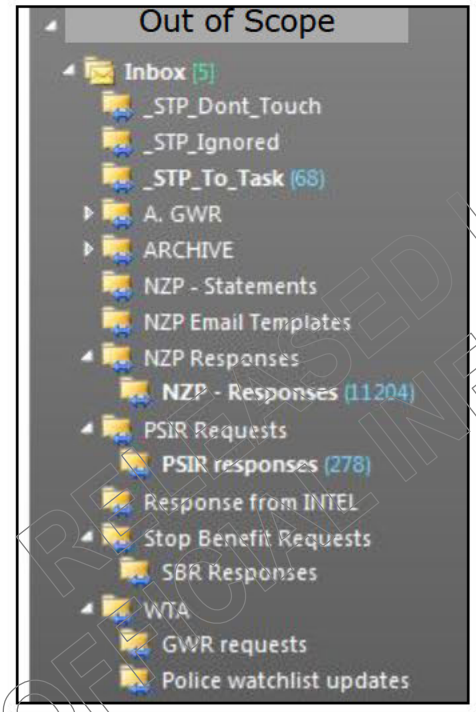
- Click 'Advanced' and 'Add'……..



- Type the newsgroup name – [redacted] and click on 'OK'



- 'Apply' the change and follow prompts until the end. The newsgroup should then appear in Outlook



The Process

Identifiers

In all cases we need to complete an identification check.

The NZ Police must provide us with at least two identifiers i.e., name and date of birth, for us to match their request for information with the client information held in CMS (although we prefer three identifiers).

Where NZ Police have not provided us with enough details to make an accurate match in CMS, we will email the requesting officer back and request further identifying information e.g., address, other known aliases.

Providing the right information

Under the Privacy Act we are given authority to release any personal information about a client if we believe there are reasonable grounds, and it is required to maintain the law.

The information we provide can include but is not limited to person details such as current and previous benefit details.

Where we are not certain why information is required and of what relevance it is to the Police, we can contact the Police Officer directly to ask why the information requested is needed, and of what relevance is has to their investigation.

Examples of information **not** provided unless a necessary reason has been specified include:

- Client Number
- Agent bank accounts
- Client's work details

An 'Official Template'

When NZ Police send requests for information, they **must** complete a formal template.

These may come in different forms; Information Request Form (IRF), General Warrant Request (GWR), Public Safety Information Request (PSIR), Stop Benefit Request (SBR).

In this template the Police should provide the following:

- Specifically state "Privacy Act Section 6 Principle 11 (e) (i & iv)
- State the name of the person, their date of birth and last known address
- Clearly advise what information is required
- The reason for the request for information
- The name, QID, Station (location) and a contact number of the requesting officer

If you receive the old email template, you will forward this back to the requesting Officer using email template below:

Hi [requesting officers name]

There have been some changes to how you will request information from Work and Income. Please note this is an old form and does not have the SEE mail signature embedded in it.

The form that you require is **Information Request form POL 4135.**

If you have any queries or questions regarding the new process, please email or contact your District Prevention Manager.

You will need to resend your request (one request per email) for processing on the new, correct Police Request form. If your request is Urgent, then please mark **URGENT** in the subject field of the email and submit for processing.

Thank you and regards,

[your signature incl. SEEMail]

If any of the above are not provided, you cannot complete the request. You will respond to the requesting officer with what is required so they can amend the RFI and return for processing.

Address information

Where our clients have a current postal address which is a *street* address, we should give both the residential AND postal addresses (where they are requesting address information), for example:

Residential address (current from 15/08/15)

s9(2)(a)

Postal address (current from 21/03/15)

s9(2)(a)

The reason we provide this information is that often the person the police are enquiring about can be contacted through residents at the postal address; therefore, we are trying to provide a better service to the police.

Postal Addresses (PO Box / Private Bag)

Where our clients have a current postal address which is either a PO Box or Private Bag, we should not give the NZ Police these details. It is not likely that the NZ Police are trying to post a letter to our clients.

C/O (care of) Addresses

If the address is C/O someone other than the client, we can provide the address but delete the name of the other person.

Emergency Housing (EH) Clients

If you have reason to believe that the client is currently in Emergency Housing (i.e.: Current benefit but address listed as 'No fixed abode'), Please provide any current Emergency Housing details (i.e.: Name of EH, Dates booked if available and address if available) as found in the Hardship assistance screen in CMS.

Collections Addresses

We will not provide any "Collections" postal addresses.

Reason for the request

***These are not complete lists. Staff must always use their discretion to determine if the requested information is necessary for the investigation to proceed.*

The following examples are enough to complete the Police Officers request:

- Investigation into a burglary
- Suspect in theft investigation
- Is in Breach of Court Bail and concerns of safety
- Client is sought for a burglary that occurred
- Client has a Warrant to Arrest (WTA) for failing to appear at the District Court
- Required to be located and spoken to in relation to two incidents of fraud
- For service of a summons to appear in court
- Wanted to serve a DNA compulsion notice on
- Drugs investigation
- Sexual Abuse
- Domestic Violence
- Traffic Offence

Insufficient reasons

The following examples require further information before a request is completed:

- Client is a victim for a serious matter and needs to be located
- Wanted/Witness to be interviewed
- Criminal investigation
- Police file number
- Active charges

If you do not feel that the reason the Police are requesting information from us is reasonable e.g., "need to talk to this person", you should email the Police to seek clarification.

Other reasons

Some Officers may ask for other information. Below is a list of common requests we have seen and the process we should follow when receiving them.

Return of Property

DO NOT provide client details for this reason. Check the client's benefit status and if current, contact the client to advise that we have received information from the NZ Police that they are holding property that belongs to them. Provide the client with the requesting Officers name and contact number to follow up further.

Calling the client: Remember to dial '25' before the client's phone number. This is so the work and income 0800 will appear instead of 'unknown number'.

Client Contact Made

- Response to requesting Officer

Hi there,

We are unable to provide you with information based on your reason for request. We have however contacted the client on your behalf and provided them with your name and contact details (as per the request form). They will contact you to retrieve their property.

Regards,

(your name)

Out of Scope

No contact made *or* Benefit Not Current: Leave a Must View Note on the client's record so that if contact is made, the client can be advised to contact the requesting Officer.

- Must View Note (Expiry Date – 1 year)

NZ Police have property to be returned to this client. If client makes contact, please ask them to enquire at the following Police station Station: Contact No: Once done, please remove the MVN.

- No Contact Made - Response to requesting Officer

Please be advised that due to the Privacy Act, I am unable to provide you with this client's details as 'Return of property' does not fall under the Privacy Act criteria. I have left a message to contact your station on the client's record.

- Benefit Not Current – Response to requesting Officer

Please be advised that due to the Privacy Act I am unable to provide you with this client's last known address. I was unable to contact this client as their benefit is no longer current. I have left a note on the client's record should they contact Work and Income in the near future.

Agents Bank Account

Advise the requesting Officer that the clients' bank account belongs to their agent and that we are unable to provide this information for this reason.

If the Officer persists, then they should provide a specific reason for this and explain how this is relevant to their enquiry. If you feel their reason is enough, seek manager's approval before providing this information.

- Response to requesting Officer

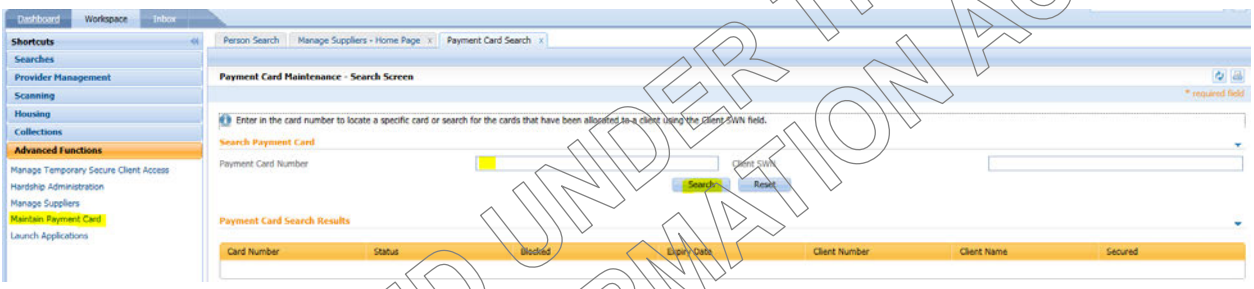
Bank account number: Unable to provide as client has no bank account listed, payments received by an Agent.

Payment Card Details

If NZ Police provide us with the full payment card number, we are able to search for this in CMS to locate client details following the below steps:

Click on the following latches/tabs:

- Workspace
- Advanced Functions
- Maintain Payment Card
    - Add Payment Card number and 'Search'
    - The client details will appear in the results field below where you can click on the client's name to open their record in SCMS



If we have a partial payment card number (i.e.: last 4 digits) then we can put the request on hold (in S2P with a note stating "Awaiting information from Intel) and email the INTEL unit at Out of Scope to follow up.

Once INTEL has provided us with the information, we will send this to the requesting Officer and pull our 'hold' record back and 'Complete'.

Note: You should remember to keep the officer informed if you are getting further information from another business unit.

Part of a Confidential Investigation

NZP must provide a sufficient reason for requesting information. If a request comes through with 'confidential', we must ask the office to clarify the nature of the investigation prior to releasing the information requested.

Note: In your response email to the Officer, you will need to CC Out of Scope so these requests can be monitored.

Statement request

After a response is sent to NZ Police they may ask for a 'Formal Written Statement' for court regarding the information that has been provided. If a request is received, we will complete the 'Formal Written Statement' template *(see appendix)*. We will send a draft copy to the officer to ensure that it meets their requirements. If the officer approves, then print off the statement on an MSD letterhead and have this signed off by a manager.

Collect the original request, response, 'Formal Written Statement' and any other relevant documents. Email a digital copy and courier a hardcopy to the requesting officer.

Should you require assistance with a statement request, please contact the following staff:

- Out of Scope

Premises visited

NZ Police may come back to us advising that they have visited the premises of the client and they no longer reside there. When this happens, we will:

a) Add the below template to the clients CE Notes and refer to the sites Ready for Processing Queue so they can follow up accordingly

> CPU has received information from NZ Police advising that this client is not residing at the address as per CMS. As this information has come from an outside agency, CPU is unable to take any action on the client's benefit. Could you please follow up with the client to ensure the address details we hold are up to date and correct.

b) Email the requesting Officer back to advise that you have followed up with the Service Centre.

Partner details

We are not authorised to provide partner details. Where this is requested, we should advise the requesting Officer to send through a new request for information, using the template below.

> Hi there,
>
> Unfortunately, we are unable to provide this information as the partner is not the prime suspect. If you require partner information, please send through a new request naming the partner and stating what and why this information is required and how this will help with your investigation.
>
> Thank you,
>
> (your name)
>
> Out of Scope

Suspend Benefit Request (SBR)

Police will make a reasonable effort to locate the person based on the information provided through a PSIR. If the person cannot be located, Police will complete a ***Stop Benefit Request*** (SBR) to request MSD to stop benefit.

All SBRs **must be** authorised by an officer of or above the level of inspector.

When CPU receives information from the Police relating to a client's outstanding public risk warrant this needs to be added manually as a Warrant to Arrest – PR in WASP.

This process will be covered in another training session. In the meantime, if you receive a Stop Benefit Request, please forward the request to the following staff:

- Out of Scope
- Out of Scope
- Out of Scope

To ensure this request is dealt with promptly, please send the request to all 3 CPOs named above or escalate the SBR request to a Centralised Services – Mangere Service Manager

Phone recordings

Occasionally the NZP may request phone calls information. In these instances, we will email the request to Out of scope who will facilitate these.

Call recordings are only stored for 90 days before they are deleted, however, the Contact Centre call logs are currently stored for at least 13 months.

Police can request call recordings either through the Contact Centre, the Region or Service Centre.

Unable to locate the client

If you cannot find the person in CMS or SWIFTT, you will respond using the template in your learner's guide:

> Hi [requesting officer's name]
>
> We are unable to locate this person with the information provided. Please advise if they are known by any other name (alias), middle names, address or DOB. Please included any updated information in the request form.
>
> Thank you and regards,
>
> [your signature incl. SEEMail]

Note: Remember to 'Forward' the email so the original Request is attached to your response.

Non-current Benefit

Where the NZ Police request information for our clients whose records are non-current (suspended/expired/cancelled/registered/declined/cond.grant), we should advise them as such.

Address information requested (non-current benefit)

"Last known address…"

Benefit status requested (non-current benefit)

"This record is not current since (date benefit stopped)"

More than one request as an email attachment

The Police quite often send two or more requests through on one email attachment. The standard process is one request per email.

You will need to forward the email back to the requesting Officer and advise that they should send one request per email – it is easier to process one request at a time and to keep track of the requests.

Police request hard copies of documents

If the Police ask for hard copies of client application forms or documentation, where this is in the clients Scanned Documents then we can provide this information. Please use your discretion on what has been requested. Do not breach the privacy of any third parties named in the scanned documents or provide any information that you wouldn't normally provide. If you are unsure, please ask for guidance.

Advise the officer that our offices do not hold /keep original copies of forms once they have been digitised.

If there is documentation required that we cannot locate in Scanned Documents, then we will refer this to the Site to follow up further.

We should respond to the Police advising them that we have forwarded their request for documentation to the Work and Income Service Centre concerned.

Response to Police: Documentation requested - forward to Service Centre

Hi [requesting officers name]

Client: [full name and date of birth]

We are unable to complete your attached request as we do not hold client documentation or files in our office.

We have forwarded your request to the Work and Income [site area name] Service Centre Manager, [SCM's name] to respond to your request under the Official Information Act.

We have advised the Manager to contact you directly regarding this matter with the contact number provided on your request.

Regards,

[your signature incl. SEEMail]

Forward Police request Service Centre Manager

Hi [SCM name]

We have received an information request from NZ Police. We are unable to complete this request as it is for documentation which your site holds.

Please find attached the request for information which the NZ Police have forwarded to us. This request should be considered under the Official Information Act.

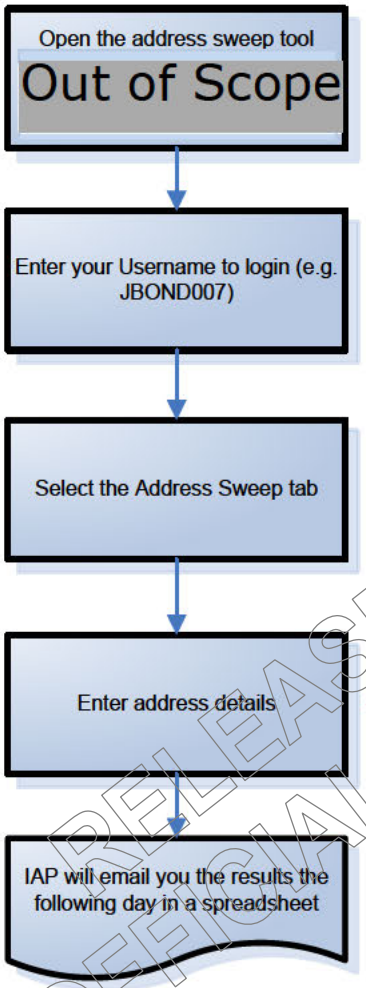
Please contact the Police Officer using the contact phone number included in the attached document as soon as possible regarding this matter.

Thank you and regards,

[your signature incl. SEEMail]

Request for Address Sweep

There are times where the Police ask for the details of "occupants of an address", this is usually referred to as an 'Address Sweep'. The 'sweep' is completed through a portal and the information is delivered to you the next day via email. To do this, follow the process below:



Note: If the client resides in an apartment or flat, we will only provide the 'house' number e.g., 71a Smith Street – we provide 71 Smith Street.

The reason we do this is because Intel cannot identify addresses in this format. *However*, Intel can identify **all** addresses with "71 Smith Street" i.e.,71**a** Smith Street, 71/**2** Smith Street etc

If the Police Officer has requested other information alongside the address sweep you should provide a response to this and advise that an Address Sweep is underway, and the information will be available within 24 hours.

Receiving the Address Sweep

The response from Intel will be returned to you (the requester). It is important that you set up an email 'rule' to identify these requests, so they can automatically move to the shared NZP email newsgroup – this is to eliminate the risk of work not being completed due to unplanned leave for example.

The information from Intel will be presented on an excel spread sheet. Do not send the spreadsheet to NZ Police. Only send relevant information.

Providing the Address Sweep information to NZ Police

Once the address sweep is received, we will need to complete the following steps before providing our response:

- Open the spread sheet and filter out the 'current' clients only
- Check that the address in the spread sheet matches the address that was provided on the original request
- Where the information is the same, provide client names in a new response to the requesting Officer
- Where the information is not the same, advise the requesting Officer as such:

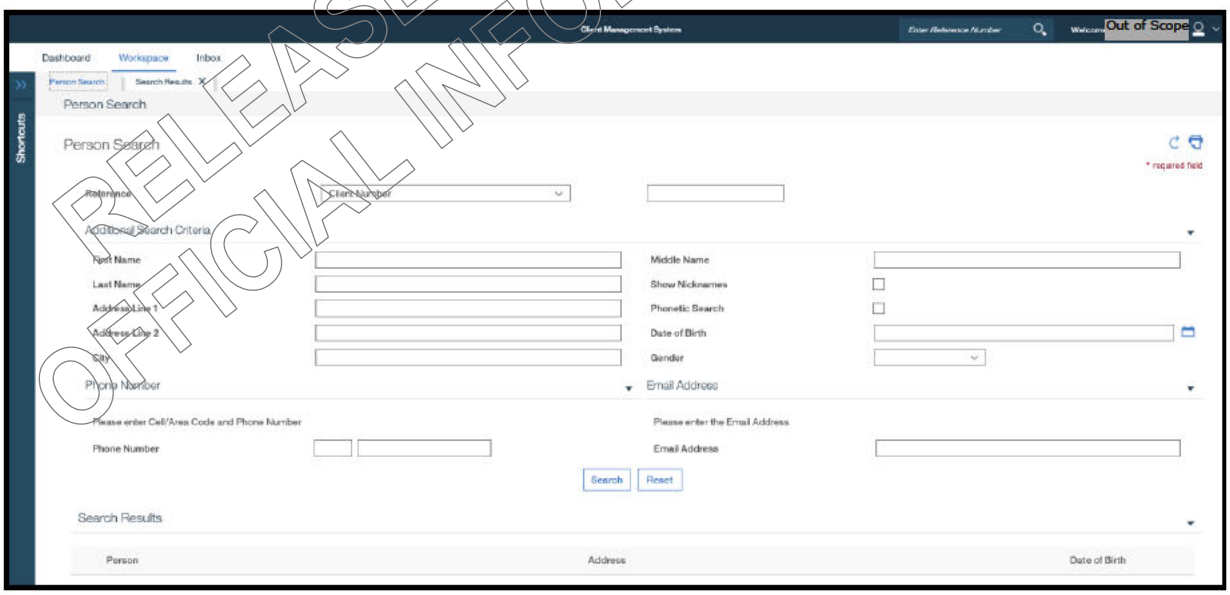
  "We have no record of any other occupants residing at the address provided"
- Where all contact details have been requested, you will need to search for the client in CMS to provide this information (address, phone, email)

Locating the information

Once we have deemed that the information requested meets the standards and at least two identifiers have been provided to locate the client, we will search their information using CMS.

In most cases, NZ Police will provide the clients full name, date of birth and last known address.

- Using the 'Person Search' function you will search for the client (or child) using the identifiers provided.



Note: If you cannot locate the client you will respond to the requesting Officer as such – "Unable to locate this person with the information provided"

Other search types

We can also search in CMS with the following functions:

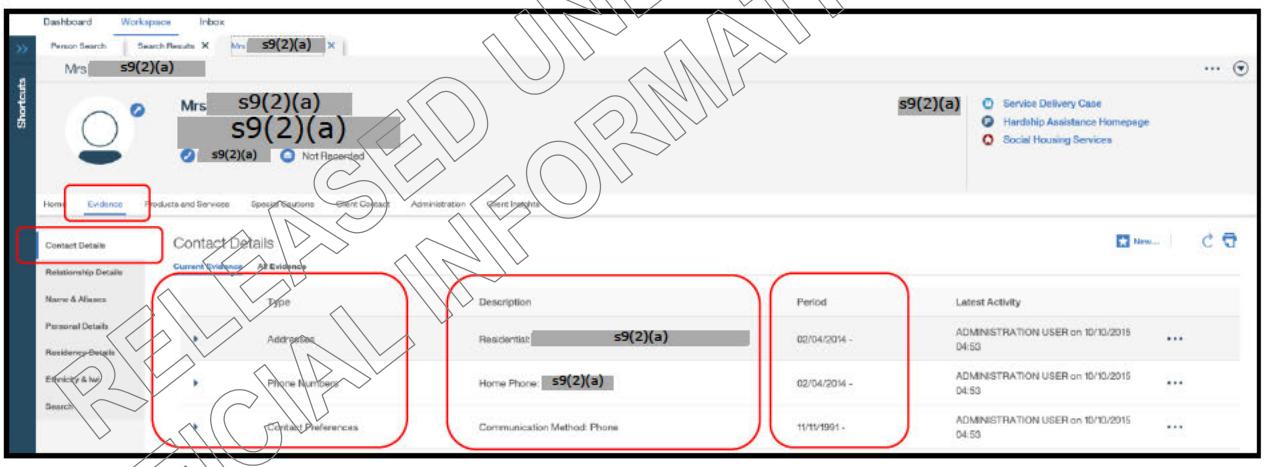
- Bank Account
- Client number
- Community Services Card number
- IRD number

Note: It is not common practice for NZ Police to request this information.

The information required for the NZ Police RFI can be found in the following sections of CMS:

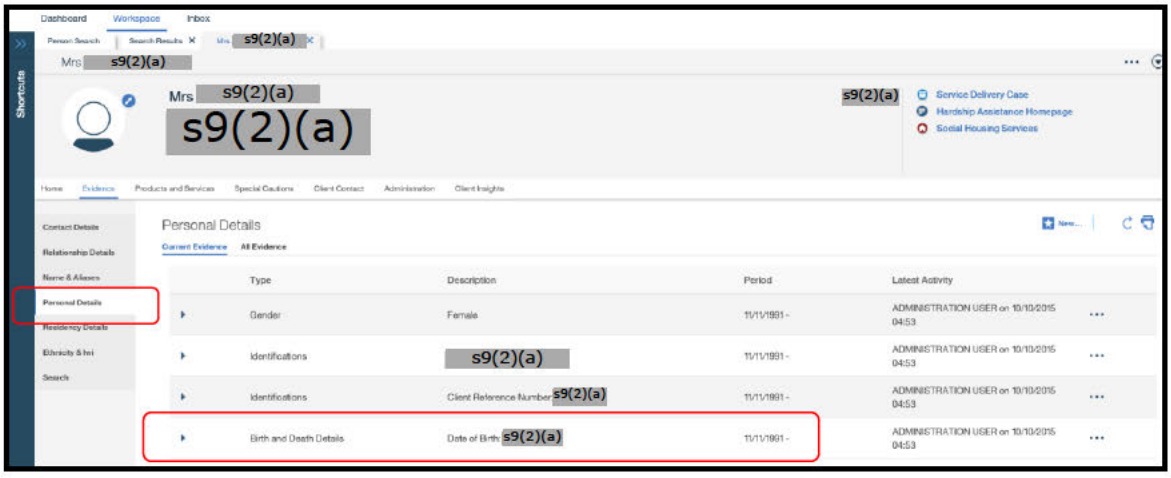
By clicking on the 'Evidence' latch you will locate the 'Contact Details' tab. Under 'Current Evidence' you will find:

- Address (residential and postal) details and the start date
- Phone number details and the start date
- Email details and the start date



Note: Previous contact details can be found by clicking on the 'All Evidence' tab

If the client is deceased, the 'date of death' can be located by clicking on 'Personal Details;



SWIFTT

To locate benefit and bank account details, navigate to SWIFTT, SSTAI screen:

```
Statutory stand-down waived
Commencement date        : 27/05/13   *52 week Reapplication not complete
Number of children       :  1
FTC/BSTC                 : FTC     92.73
Service type             : SPS              Current     27/05/13    313.65
Supplementary allowance  : AS               Current     29/05/13     20.00
                         : WEP              Current     01/07/18     31.82
                         :
                         :
Next Review/52 wk Reapp  : 25/05/03                                  Income:   168.00
Next pay day             : 16/04/19 TUESDAY     448.20               Expiry:
Date last action         : 23/06/18 USER NOT KNOWN                   Debts :
Bank reference           :  s9(2)(a)                                 Payees:Y
Comments                 :                                           Agents:
```

Note: If the Agent field (bottom right) has a [Y] check the SPYHI screen to ensure you are providing the clients bank account details and not the agent – CL for client and AG is Agent (example below).

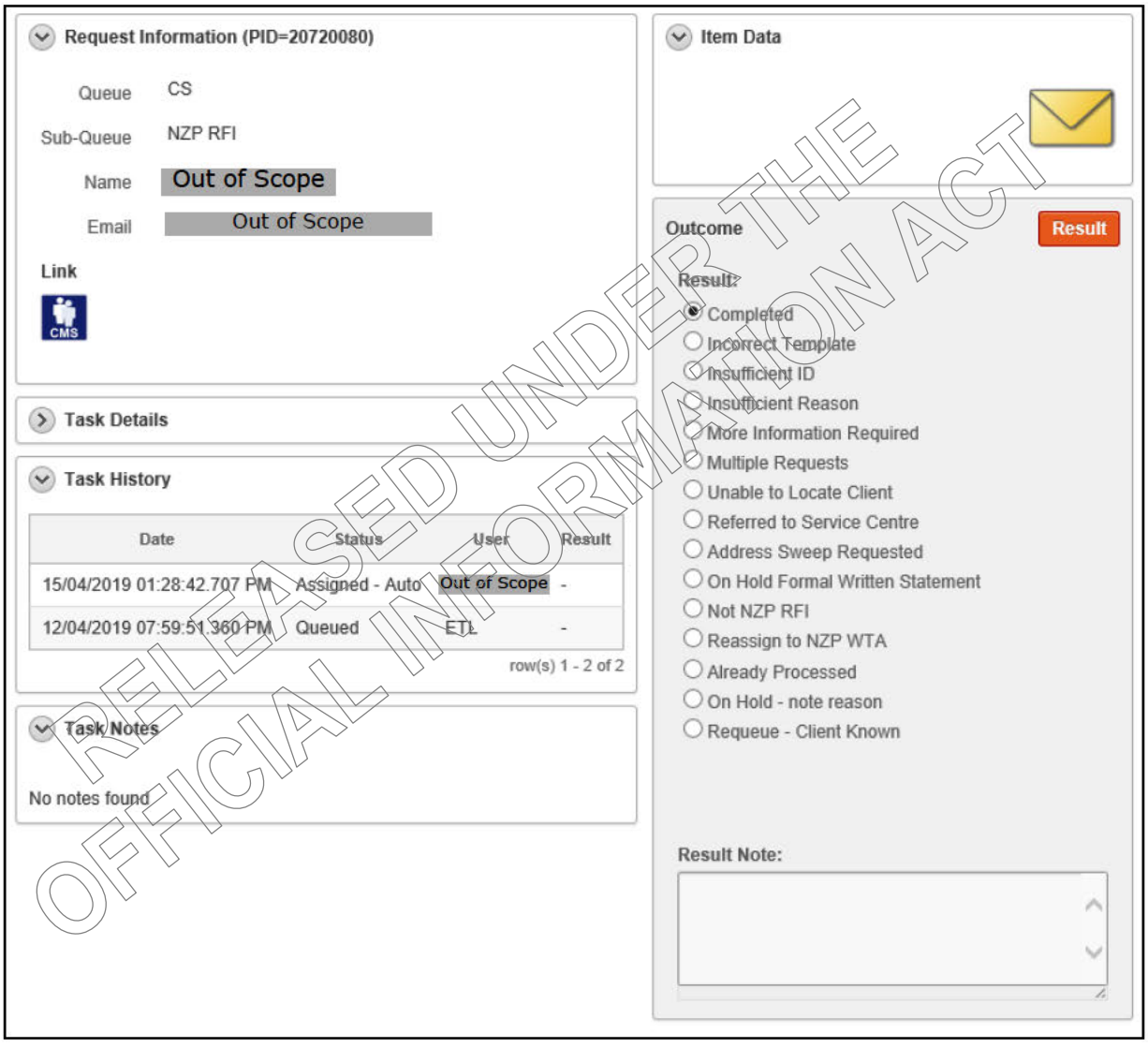
	Pay date	Day	Service	Due	Issued	To
1	06/10/16	THU	EMA1	241.51	320.51	CL

To

Straight to Processing Tool

The NZ Police Requests for Information are managed through the Straight to Processing Tool (S2P). Staff who are assigned to the NZ Police work queue will be 'pushed' work for processing.

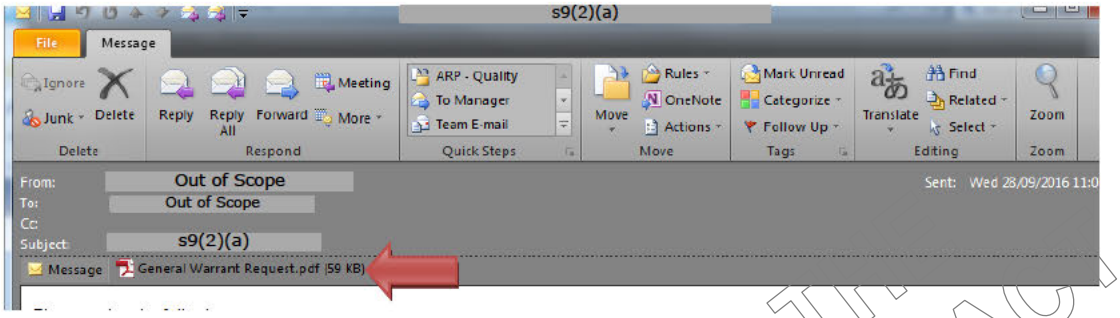
Below is a screenshot of what this work looks like in S2P:



Opening the Request for Information

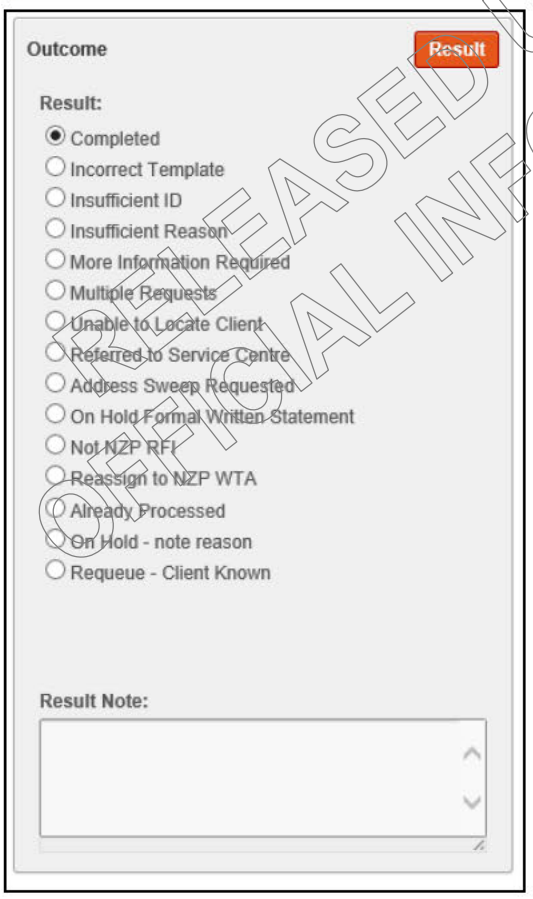
To open the RFI in Outlook you will need to click on the envelope displayed in the 'Item Data' field in S2P.

Click on the attachment to review the RFI.

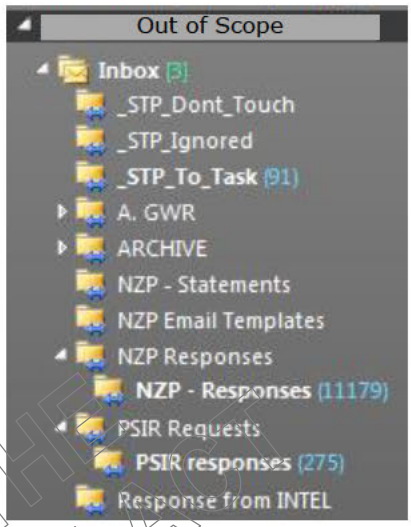


Resulting S2P

Once you have completed your response, you will select the Outcome that reflects the action you have taken and click on 'Result'.



Filing Response emails

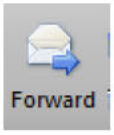


Once you have sent your response email and 'resulted' your action in S2P, these should be filed for audit purposes.

Staff are encouraged to use the Outlook rule/alert for completed requests to be automatically moved into the correct response newsgroup however if you do not have a rule/alert in place, you will need to manually move the response email from your personal sent box, and move it into one of the following folders in the NZP newsgroup:

- NZP – Statements (Statement response emails)
- NZP – responses (General RFI's responses)
- PSIR responses
- Responses from INTEL - Address Sweep emails

How we respond



When responding to RFI's, we click on the 'Forward' button in our email; this is so the request is attached to the response, and we will respond in the body of the email.

This makes it easier to locate all the information at once, rather than having requests and responses in different folders. This is also for auditing purposes.

Completed Requests

Once we have completed the request for information, we must ensure that we are "filing" our requests into the appropriate folder.

Filing the NZ Police requests in the appropriate folders is our electronic form of "batching" for this area of work.

Request for Suspension

At times the NZ Police advise us that a person is not residing at the address we have provided them. Based on this reason, the NZ Police may request we suspend the clients Accommodation Supplement (AS) or Main Benefit.

Where this happens, we will first need to search and locate the client in CMS to determine if the person is currently receiving assistance from Work and Income (Products and Services latch in SCMS or SWIFTT SSTAI screen).

If Accommodation Supplement is currently being paid for the address we provide, and the Police confirm the person is not residing here, we will need to refer this request to the Service Centres Ready for Processing Queue (RFPQ) through CMS and ask them to follow up and respond to the Police Officer to advise that we are unable to suspend the benefit but have referred this to the site.

Referring to the sites Ready for Processing Queue

To refer this information to the site we need to create a Client Event Note using the template below:

- Business Group: Service Delivery
- Event Type: Change in Circumstances
- Event Sub-Type: Other
- Description: NZ Police RFI – client not at address

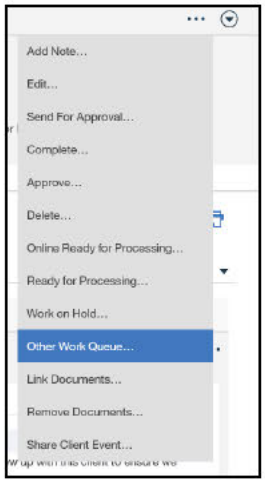
If it is a Seniors (NZS) client, you will select 'Seniors' as the Business Group

CEN Template

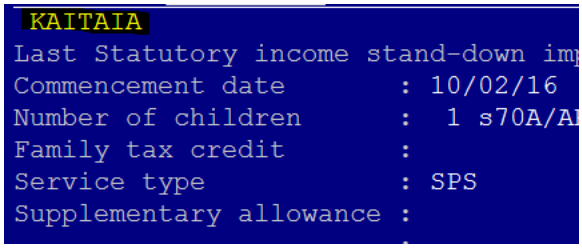
CPU has received information from the NZ Police that this client is not residing at the address as per CMS. As this information has come from an outside agency CPU is unable to take any action on the clients benefit. Could you please follow up with this client to ensure we have the correct address or amend accordingly.

Note: If you have selected 'Seniors' as the Business Group, because the client is in receipt of NZS/VP, the note will automatically be referred to the Seniors Ready for Processing Queue. **You will not need to complete the next steps.**

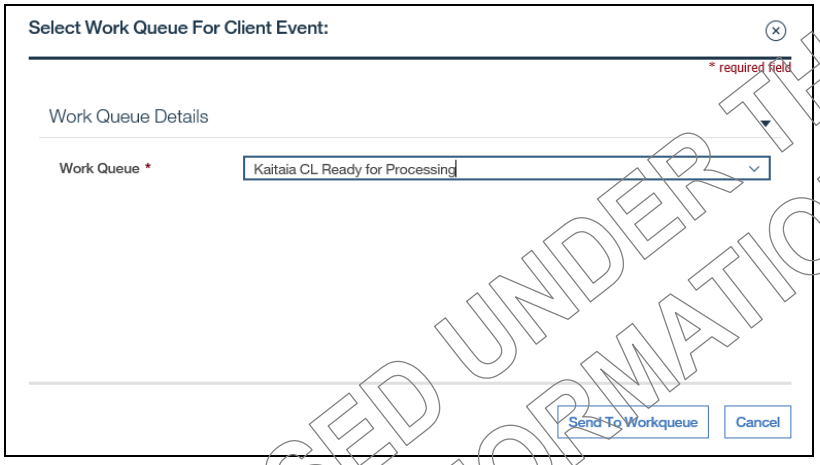
Click on 'Action' and select 'Other work Queue'



Select the sites Ready for Processing Queue (refer to SWIFTT SSTAI screen for site details)



Click 'Send to Workqueue'



Why we don't suspend

The person in question may be actively avoiding the authorities but do in fact still reside at the address we have on our system.

In these instances, we should always refer to the site so they can follow up with the client to give them the opportunity to correct our records before we undertake any suspension based on advice from NZ Police, or any other outside agency.

Live Actions

Notes:

Notes:

Quality and Assurance

Share

Your work will be 100% checked until deemed competent, this means you are able to process the work independently and the accuracy of your actions are 95% or more (Advise learners of who their support person is if it is not you i.e., Quality Assurance Officers).

Once competent, your work will be randomly checked each month by the Training & Quality team.

Appendix

Appendix 1 : Response/Email/CEN templates

General RFI response layout for IRF (in body of email)

Note: Edit fields as required – only provide what is requested

Our Response:

[Client name]

[List information requested by Officer]

- If we state **'Last Known'** – that indicates they are not receiving current assistance from MSD.
- If your request is Urgent, then please mark **URGENT** in the subject field of the email and submit for processing.

[your signature incl. SEEMail]

General RFI response layout for GWR and PSIR (in body of email)

Note: Edit fields as required – only provide what is requested

Benefit status: [current, suspended, cancelled, no record]

SWN:

Current (or Last Known) address:

Date registered at address:

Contact phone number(s):

Date phone number registered:

Future appointments: [date, time, location]

Bank account number:

Any other information: [only complete if specific information requested in PSIR]

[your signature incl. SEEMail]

Email templates

Response to Police: Insufficient reason for request

Hi [requesting officers name]

Client: [full name and date of birth]

We have not responded to your request for information as the reasons you have provided are insufficient.

Please resend your request with more specific reasons as to why you require this information.

Thank you and regards,

[your signature incl. SEEMail]

Response to Police: Incomplete template

Hi [requesting officers name]

Please resend the attached request with **all** information provided, including:

- the reason for your request and
- Your Officer information.

Thank you and regards,

[your signature incl. SEEMail]

Response to Police: One request per email

Hi [requesting officer's name]

Please resend the attached request as two *separate* requests. One request per email.

This makes the process faster and easier to keep track of.

Thank you and regards,

[your signature incl. SEEMail]

Response to Police: Documentation requested - forward to Service Centre

Hi [requesting officers name]

Client: [full name and date of birth]

We are unable to complete your attached request as we do not hold client documentation or files in our office.

We have forwarded your request to the Work and Income [site area name] Service Centre Manager, [SCM's name] to respond to your request under the Official Information Act.

We have advised the Manager to contact your directly regarding this matter with the contact number provided on your request.

Regards,

[your signature incl. SEEMail]

Forward Police request Service Centre Manager

Hi [SCM name]

We have received an information request from NZ Police. We are unable to complete this request as it is for documentation which your site holds.

Please find attached the request for information which the NZ Police have forwarded to us. This request should be considered under the Official Information Act.

Please contact the Police Officer using the contact phone number included in the attached document as soon as possible regarding this matter.

Thank you and regards,

[your signature incl. SEEMail]

Response to Police: When submitting incorrect forms etc.

Hi [requesting officers name]

There have been some changes to how you will request information from Work and Income. Please note this is an old form and does not have the SEEmail signature embedded in it.

The form that you require is **Information Request form POL 4135.**

If you have any queries or questions regarding the new process, please email or contact your District Prevention Manager.

You will need to resend your request (one request per email) for processing on the new, correct Police Request form. If your request is Urgent, then please mark **URGENT** in the subject field of the email and submit for processing.

Thank you and regards,

[your signature incl. SEEMail]

Response to Police: Follow up required - Client not at current residence

Hi there,

Client: [full name and DOB]

We are unable to comply with your request as we cannot lawfully suspend any part of a benefit for the purpose of obtaining information on behalf of another agency.

I have however contacted the Service Centre the client deals with and requested that they attempt to establish the client's current address so please consider making a further address request to us using the email address below, when it may be possible to provide you with updated information.

Out of Scope

Thank you and regards,

[your signature incl. SEEMail]

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Client Event Note Template

Case Manager follow up required – Client not at current residence

Hi [CM's name]

Client: [full name, DOB and SWN number]

We have received information from NZ Police advising that the above-named client is no longer residing at the address stated in CMS.

As this information has come from an outside agency, we are unable to take any further action.

Please follow up with this client to ensure the details we have on file are correct and/or update their address details accordingly.

Thank you and regards,

[your signature incl. SEEMail]

REMEMBER: ALL CLIENT RELATED QUERIES MUST BE ADDED TO THE CLIENTS SERVICE CENTRE READY FOR PROCESSING QUEUE.

Appendix 2: 'Formal Written Statement' Template

IN THE MATTER of Section 82 of the Criminal Procedures Act 2011

FORMAL WRITTEN STATEMENT

I, NAME state:

1 **My full name is** NAME**.**

2 **I am a Service Manager at Centralised Services (CS) in Mangere, Auckland. Centralised Services is the processing arm of Work and Income which is part of the Ministry of Social Development.**

3 **On the** Date of request**,** Officer Name **of the New Zealand Police requested Work and Income access our records and provide information held for** NAME**, date of birth** DOB**. This request was made under Section 6 principle 11(e) (i) and (iv) of the Privacy Act 1993.**

4 **The following information was provided on** DATE **to** OFFICER NAME**.**

5. **The information was extracted from the Work and Income computer database system called Single Client Management System (SCMS) and reflects the details held for** NAME **.**

I confirm the truth and accuracy of this statement. I make the statement with the knowledge that it is to be used in court proceedings. I am aware that it is an offence to make a statement that is known by me to be false or intended by me to mislead.

Signed: _____ **Date:** _____

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Intelligence Unit

Requests for Information from external agencies

Business Process 08 February 2022

Owner: Steve Bates, Manager, Intelligence and Integrity Insights Unit

Author: Out of Scope

Version: 4

Objective Reference: A13850497

Release date: 08 February 2022

Sign off

This form records the approval and acceptance of the following document:

Name	Role	Signature/Date
Steve Bates	Manager, Intelligence and Integrity Insights Unit	8/2/22
Caveats:		

Les Maxwell	Principal Intelligence Analyst, Intelligence and Integrity Insights Unit	08/02/2022
Caveats:		

Table of Contents

Purpose

To document the processes the Intelligence and Integrity Insights Unit (Intel) will use to manage Requests for Information (RFI's) from external law enforcement agencies.

Providing clear, consistent and thorough guidelines for the handling of RFI's will ensure that information is shared carefully, consistently and in an auditable manner.

This document should be considered a living document where any changes to the process are recorded and signed off by the Manager, Intelligence and Integrity Insights Unit.

Background

Intel is part of Integrity and Debt, and is responsible for the receipt and response to RFI's from various other agencies, including, but not limited to:

- NZ Police
- Department of Internal Affairs
- Ministry for Primary Industries
- Accident Compensation Corporation
- Department of Corrections
- Ministry of Business, Innovation and Employment

Process steps

RFI's are expected to be made in writing, and are generally sent to the Intel shared inbox Out of Scope either by the requesting agency themselves, or via another MSD unit. Any that are received by another Intel staff member directly are to be forwarded to the inbox, to be managed centrally.

Receipt and Triage

1. The Senior Intelligence Analyst (SIA) will create an Objective file for each request, where all correspondence relating to that request will be stored.
2. They will check the RFI to identify any potential concerns. They also need to ensure that:
   - the information required is itemised clearly
   - the 'Period of Interest' is clearly defined, and logically explained
   - there is sufficient detail to illustrate that the information requested is relevant and necessary for the agency's investigation.
   - there are no obvious legality concerns or other risks presented
   - any urgency for the request is taken into consideration

3. If there is a lack of clarity with any aspect of the RFI, the SIA will communicate with the requestor to ensure that appropriate amendments are made before the process can continue.
4. Any risks identified will be escalated to the Intel Manager, and if there are legal implications this will be discussed with the appropriate internal teams.

Allocation

5. A copy of the sent email will be stored in the Objective folder.
6. All details pertaining to the RFI will be entered into the 'RFI Tool' (http://isweb/RFI/index.asp?id=70)
7. The SIA will forward the original email, along with any directives, or concerns they have identified, to an Intelligence Analyst (IA), adding the Objective reference to the subject line.

Collation

8. IA's will seek the information requested via Ministry systems, and if further details are required from the requestor during the collation stage they will correspond with them directly. They will seek advice from a senior member of the Intel team, if at any stage they are unsure of how to proceed.

Response

9. A template, A12186519, has been designed for the response stage. IA's will complete this document, choosing the appropriate security classification. When they are ready to respond to the RFI, the IA will forward the email they received, along with their response attachment, to the shared Intel inbox.
10. The SIA compares the original RFI with the proposed response, to ensure that the information to be provided matches what was requested only, to avoid the risk of over- or under-sharing of information.
11. The SIA saves a copy of the IA's email to the Objective folder.
12. They forward the response, less any internal correspondence, to the requestor using the Intel inbox as the return address.
13. The SIA will complete the 'response date' field in the RFI Tool, and save a copy of the final response into Objective.

14. All emails relating to the request will be added to the agency folder in the Intel inbox. This ensures that two copies are retained, in the event of office or technology error.

In the absence of the SIA, their tasks will be completed by Intel's Principal Intelligence Analyst (PIA).

Reporting and Monitoring

Recordkeeping

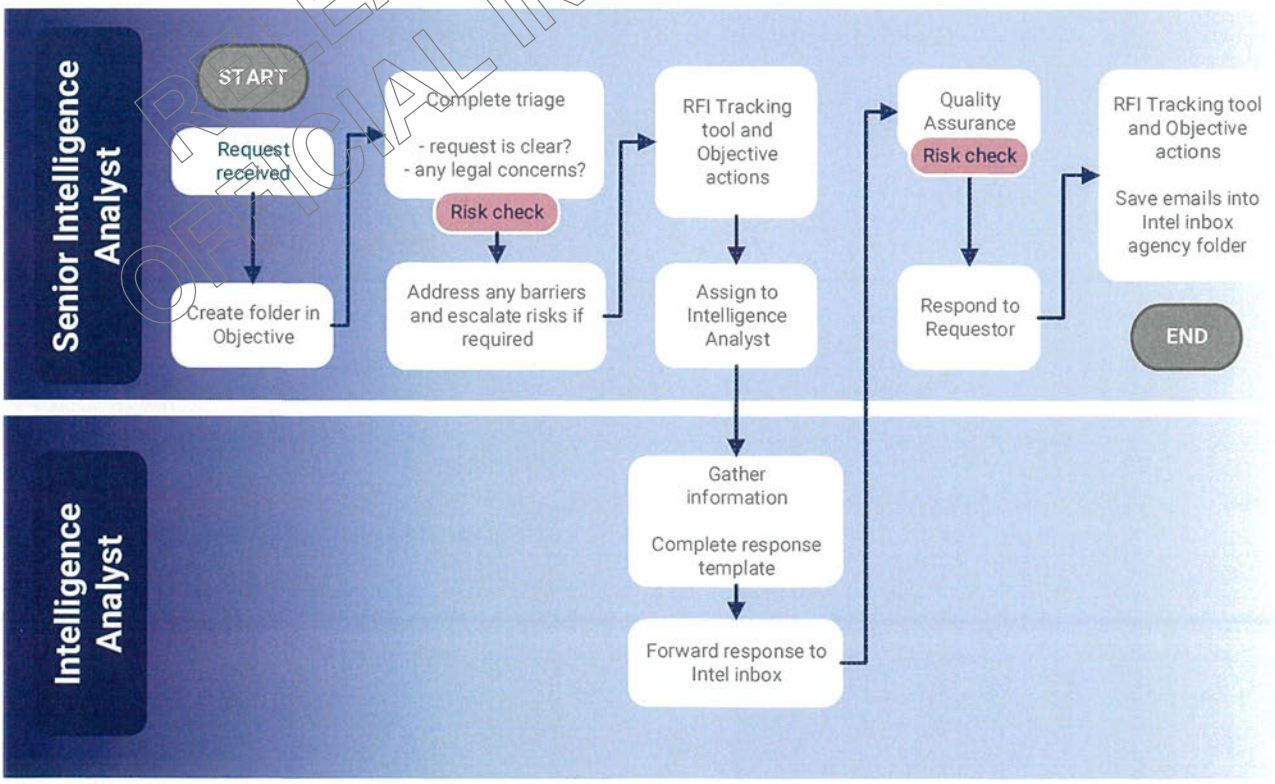
All requests and responses must be recorded in the RFI Tool. All supporting evidence and responses provided (such as emails and attachments) must be retained and stored in Objective.

Auditing and reporting

The Manager, SIA, and PIA will be able to use the RFI tracking tool to complete quality checks, monitoring and reporting on all RFIs received by Intel.

RFI Process Flowchart

This diagram visually illustrates the business process:



Operating Protocols for sharing information with the Gang Harm Insights Centre

19 October 2023

Table of Contents

Protocol Sign off

The Operational Protocols are authorised by:

Debbie Power — Date: 26/10/23

Chief Executive, Ministry of Social Development

Introduction

The Ministry of Social Development (MSD) has agreed to be bound by the terms and conditions contained in the "Information Sharing Agreement between the New Zealand Gang Intelligence Centre Agencies" (the AISA) dated 7 November 2018.

The Gang Intelligence Centre (now known as Gang Harm Insights Centre)[1]. was established to enable a multi-agency approach to address problems caused by gangs and to reduce the harm they cause to communities through shared intelligence-gathering, enhanced law enforcement, prevention, intervention, and rehabilitation. The Approved Information Sharing Agreement between the New Zealand Gang Intelligence Centre Agencies, now the Gang Harm Insights Centre Agencies, (the AISA) was approved by Order in Council as an Approved Information Sharing Agreement under part 9A of the Privacy Act 1993 and came into effect on 4 January 2019.

These Operational Protocols contain more detailed operational information than is possible in the AISA. Specifically, it will be information that may require updating over time and while subject to the terms of the AISA is normally the responsibility of Chief Executives with respect to the operation of their agency. Defined terms in the AISA will have the same meaning if used in these Operational Protocols.

These Operational Protocols (and subsequent revisions, apart from minor changes that have no privacy implications) were, and will be, consulted with the Privacy Commissioner before they are agreed or amended and signed by the Chief Executives or their delegate.

The Operational Protocols specify:

1. A list of information MSD may share with the NZ Gang Harm Intelligence Centre (GHIC).
2. Contact information for the Single Points of Contact and Departmental Representatives.
3. Operational arrangements (processes and procedures) that meet the intent of the Security Provisions and other Safeguards described in clauses 11 and 12 of the AISA.
4. Other information relevant to MSD's Operational Protocols for sharing information appropriately and in accordance with the terms of the AISA.

[1] The Gang Intelligence Centre formally changed its name to Gang Harm Insights Centre in September 2022.

Overview of Information Sharing

MSD will only share Information with the GHIC where the information is shared for the purposes and objectives specified in clause 1 of the AISA.

Purpose

The purpose of the AISA is to enable the parties to share Information and Intelligence to reduce Gang-Related Harm and achieve the objectives of the AISA.

The AISA authorises the Sharing of Personal Information between the GHIC Agencies and the GHIC to:

a) enable a more collaborative, cross-agency approach to preventing or reducing harm to individuals, families, communities, or society generally that is caused by, or contributed to by, the activities of gangs; and
b) enable the enforcement of the law; and
c) produce data on crime trends.

Objectives

The objectives of the AISA are to:

a) improve Government's effectiveness at reducing the Gang-Related Harm and gain efficiencies through more collaborative, cross-agency work, and improved combined intelligence;
b) reduce Gang-Related Harm to gang members, their families and communities through early intervention (including through activities that prevent Gang-Related Harm), the provision of targeted social services and managing compliance with social obligations to support affected gang members, their family members and affected individuals in the community, especially vulnerable children and young persons;
c) prevent and reduce the level of Gang-Related Harm suffered by individuals and New Zealand society generally from Gang Criminal Activity through improved enforcement activities including detection, investigation, and prosecution; and
d) enable sufficient protection of people's privacy and ensure an appropriate balance between security and transparency when Sharing Information under the AISA.

As set out in clause 2 of the AISA, "Operational Overview":

- MSD may share information with the GHIC to contribute to the NGL as a regular, transactional share facilitated by MSD's Intelligence and Integrity Insights team
- MSD may share information to request GHIC Intelligence Products from the GHIC, or with the GHIC at the request of the GHIC for the purpose of developing Intelligence Products
- The GHIC may share information and Intelligence Products with MSD in response to a request, or proactively if relevant to MSD's functions.

MSD cannot be compelled to provide information and may place constraints on information provided.

MSD may also decline to provide information requested by the GHIC at its discretion, including where MSD determines that the request does not meet the purposes or

objectives of the AISA. This may be, for example, because it is intelligence about an individual who is not a member of a New Zealand Adult Gang nor associated with one.

MSD may put constraints and conditions on certain Information, Intelligence or data types provided to the GHIC. This may include but is not limited to where disclosure of information may cause harm to, or affect the wellbeing of, MSD clients or breach existing relationships of trust.

The AISA does not enable or require the GHIC agencies to share information with each other except where already permitted by existing law or information sharing arrangements.

Information that may be shared

Information that may be shared under the AISA by MSD will be Information that falls into the categories in the table below and is provided at the discretion of MSD.

All categories of Information (personal and non-personal) may include raw data, Intelligence, copies of official documents, forms or applications submitted and alerts. Information shared may be about any Gangs, Gang Members, Gang Associates and Victims.

Information Category	Description
Assets	Information about any real and personal property held, or in which an interest is held, by an individual or an organisation or entity, including cash as defined in section 2(1) of the Financial Transactions Reporting Act 1996, in bank accounts, accounts in financial institutions, shareholdings and beneficial interests in trust.
Contact Details	Information that may be used to contact an individual or entity (such as addresses and phone numbers), including information about any other individual recorded as being a contact individual for that individual. This includes current and historical Information, and preferred language(s) for contact. Information that identifies, and may be used to contact, the next- of-kin of an individual who is a Gang Member or Gang Associate.
Criminal Investigations	Information relating to any criminal investigation conducted in respect of an individual, including any criminal charge that has, at any time, been laid against an individual, whether or not that charge resulted in a conviction. It includes investigative findings and information collected in respect of investigations under Social Security Act 2018, Oranga Tamariki Act 1989 and Crimes Act 1961 including fraud allegations and allegations of family violence.
Education	Information relating to an individual's education history including that supplied in travel documentation. This includes training programmes, qualifications, and curriculum vitae.
Employment	Information relating to an individual's current or previous employment including:

	(a) an individual's current or previous engagement in a contract of service or a contract for service; (b) the parties to such a contract; and (c) any other Information relevant to the engagement (including information about benefits, subsidies and entitlements).
Family Relationship	Information about any person (person B) with whom an individual has, or has had, a family relationship. Person B includes another person who is or was a spouse or partner of the individual, is or was a child of the individual or their spouse or partner, is or was a family member of the individual or ordinarily shares or shared a household with the individual. "Family Relationship Information" means Information about a Family Relationship and includes information about Person B: (a) the current and previous names and other Identifying Information including aliases, contact details and dates of birth; (b) Information about the Assets and Liabilities; and Employment Information, Social Assistance Information, Financial Transaction Information and Tax Information.
Financial	Basic financial Information relating to an individual including details of bank accounts (such as bank account numbers), income, entitlements, benefits and subsidies, debt, living expenses, indicators of hardship..
Financial Relationship	Information relating to an individual's business or financial relationship with, interest in or other linkage to, one or more individuals, organisations or entities. "Financial Relationship Information" means Information about a financial relationship and includes: • the current and previous names and other Identifying Information including aliases, contact details of individuals with whom an individual has a financial relationship and the dates of birth of those individuals; • Information about the Assets of those individuals; • Employment Information, Financial Transaction Information and Tax Information about or concerning those individuals; • Any monetary payment authorised or made as Social Assistance and received by, or on behalf of, individuals, including main benefits, subsidies, allowances, grants and other such assistance; and Information about the Assets of, and Financial Transaction Information regarding, organisations and entities with which an individual has a financial relationship.
Financial Transaction	• Personal Information or non-Personal Information relating to a movement of Assets and Liabilities or an agreement to move Assets and Liabilities and includes payments of benefits, subsidies, entitlements and allowances, and recovery of over-payments including payment methods.
Gang Associations	Information about an individual's association with a Gang.

Health and Disability	Information relating to an individual's health and disability including that supplied in travel documentation. This includes mental health Information, drug tests, and alerts for communicable diseases or exposure to dangerous chemicals.
Housing	Previous or current housing Information about an individual including: • rental payments and agreements; • other household members (key details including contact details) in a tenancy at the time the individual resided in the property; • any damage caused to the property at the time the individual resided in the property and remediation costs involved; • account information related to the tenancy the individual resided in including rent, income related rent and damage reparations; • business actions created against the individual or any household members at the time the individual resided in the property including for anti-social behaviour and complaints; • any information about gang members that will assist in preventing placement of competing gang members together; any CRIP (Community Resettlement and Integration Programme - Customer Risk Indicator Profile) information on the individual and on the tenancy at the time the individual resided at the property; and forwarding addresses.
Identifying	Information that identifies, or relates to the identity of, an individual including an individual's biographical details (including date and location of birth/death), previous names and aliases, biometric information, unique identifiers assigned by any government agency (NZ or foreign), and distinguishing features (including tattoos, or body modifications). • This information can be obtained separately or in conjunction with other Information.
Immigration	Information about an individual's immigration history and current status. This includes Information relating to visa applications, visa decisions, correspondence, and associated entities. It also includes Information relating to verification, compliance, investigation and intelligence activities undertaken in relation to an individual's immigration status (or any entities associated to that individual), including as a result of powers granted by the Immigration Act 2009 or arising from and relating to allegations and other information received from the public
Social Assistance	Information relating to an individual's current and previous Social Assistance status, entitlement, debt, Liabilities, payments and balance. It includes any benefit (monetary or non-monetary), allowance, grant, subsidy, supplement, child support, student loan or Working for Families Tax Credit.

Tax	Information relating to an individual's current and previous tax affairs and current and previous tax position including customer type (for example, salary and wage earner, self-employed, business owner), income, tax paid, tax refunds, tax adjustments, Liabilities and expenditure of an individual taxpayer or entity.
Threat or risk to safety of others	Personal Information or non-Personal Information relating to an individual that may give rise to concerns about the safety of any other person including GHIC Agency employees and agents. It includes specific alerts not necessarily covered in other categories such as for the presence of dangerous animals, firearms, explosives, dangerous chemicals or other hazards.
Travel, Movement and Location	Information associated with the movement of an individual or their Assets or Liabilities across the border such as passport, visa, and ticketing Information, declarations, passenger associations and interactions with border staff. Also includes Information about the location, movements, and travel of an individual within New Zealand.

How information is to be shared

MSD requesting information from the GHIC

Any RFIs must be in relation to two or more GHIC agencies; otherwise, the request will be rejected by the GHIC with the instruction to engage with the relevant agency directly.

Where an MSD staff member identifies a need for information from two or more GHIC agencies, or for a GHIC-produced intelligence product, the person requiring the information fills in the RFI form (see appendix) and sends it to the SPOC.

Before approving the RFI, the SPOC will consider:

- Is the information requested within the scope of clauses 6 and 7 of the AISA?
- Is the information being requested for a purpose and objective specified in clause 1 of the AISA?
- Is the request relevant, reasonable and proportionate in the circumstances?
- Is the scope of the request sufficiently clear, or is any further information required to clarify the scope of the request?
- Are there any conditions relating to the requests, any particular timeframes for response, etc.?

If the SPOC considers the request may raise privacy concerns, they will contact the Information Group Manager – Advisory Services for support.

Once the SPOC has approved the RFI the SPOC will send the completed form from Out of Scope [or other specified email] to Out of Scope [or other specified email] using SEEMail.

The SPOC will record the request on a spreadsheet in secure folder location in Objective, including information requested, date of request, any notes from consultation with Information Group, and any emails sent and received in relation to the request.

Information received from the GHIC will be stored in a secure folder in IAP under the control of the SPOC and provided to the individual requesting it with any constraints on its use that the GHIC have stipulated.

Proactive disclosures of information by MSD to the GHIC

Proactive disclosures will be made to the GHIC using SEEMail from the same inbox used for RFIs. As with the RFI for requesting information from the GHIC, the person wanting to provide the information should send it through to the SPOC with the appropriate confirmation from Information Group as for an RFI.

Before approving the disclosure, the SPOC will consider:

- Is the information requested within the scope of clauses 6 and 7 of the AISA?
- Is the information being requested for a purpose and objective specified in clause 1 of the AISA?
- Is the request relevant, reasonable and proportionate in the circumstances?
- Is the scope of the request sufficiently clear, or is any further information required to clarify the scope of the request?
- Are their any conditions relating to the requests, any particular timeframes for response, etc.?

GHIC requesting information from MSD

Where the GHIC identifies a need for information from MSD the person requiring the information fills in the RFI form (see appendix) and sends it to the SPOC.

Before approving the RFI, the SPOC will consider:

- Is the information requested within the scope of clauses 6 and 7 of the AISA?
- Is the information being requested for a purpose and objective specified in clause 1 of the AISA?
- Is the request relevant, reasonable and proportionate in the circumstances?
- Is the scope of the request sufficiently clear, or is any further information required to clarify the scope of the request?
- Are there any conditions relating to the requests, any particular timeframes for response, etc.?

If the SPOC considers the request may raise privacy concerns, they will contact the Information Group Manager – Advisory Services for support.

Once the SPOC has approved the RFI the SPOC will send the completed form from Out of Scope [or other specified email] to Out of Scope [or other specified email] using SEEMail.

The SPOC will record the request and response on a spreadsheet in secure folder location in Objective, including information requested and provided, date of request, any

notes from consultation with Information Group, and any emails sent and received in relation to the request.

Transfer of GHIC AISA Personal Information within MSD

Where MSD is holding Personal Information collected under the AISA it may share that Information, for the purposes and objectives of the AISA as set out in Clause 1, with another part of MSD and the SPOC will be responsible for taking reasonable steps to ensure that:

- the Information is only provided to staff with an appropriate justification for receiving it;
- The Information is protected against unauthorised use, modification, access and disclosure; and
- Information that is obtained with specific restrictions on how it is used is only shared in accordance with those restrictions.

Disclosure

Neither MSD nor the GHIC will disclose Information obtained under the AISA to other agencies including other GHIC Agencies unless that disclosure is either required by law, or both:

- permitted under the terms of the AISA; and
- subject to any lawful constraints applied by the GHIC Manager (which may reflect any constraints imposed by the originating agency).

Use of Information

MSD may only use Information it receives from the GHIC, including the Information contained in GHIC Intelligence Products, to support the purposes of the AISA within MSD. The information that the GHIC collects, including from the GHIC Agencies, may be used to support the purposes of the AISA including to:

- Compile and operate the GHIC List and supporting documentation
- Identifying existing or potential Gang-related Harm
- Identify individuals involved in, causing, or affected by Gang-Related Harm (e.g., victims, offenders, witnesses)
- Identify lines of inquiry into Gang-Related Harm
- Compile Information into a GHIC Intelligence Product in response to a request from a GHIC Agency for Intelligence to support the prevention, detection or investigation of offending or informing decisions about enforcement actions and interventions related to Gang-Related Harm
- Identify potential Victims or offenders of Gang-Related Harm to enable activation of preventative measures
- Provide GHIC Intelligence Products and Information to GHIC Agencies to enable them to reduce Gang-Related harm to Gang Members, families and communities, including reducing long-term welfare dependence, increase employment, improve outcomes for the children of Gang Members, reduce inter-generational

involvement, improve access to education, health and social assistance programmes, and reduce re-offending.

MSD may use GHIC Intelligence Products to produce anonymised or statistical information that may be used for monitoring, research, and evaluation.

Restrictions

Neither MSD nor the GHIC will use any Information obtained under the AISA for any purpose other than as set out in the AISA.

No GHIC Agency or the GHIC will use any information obtained under the AISA except as required by constraints notified by the GHIC to the receiving GHIC Agency.

Restrictions do not apply from the point in time (if any) that the Information becomes publicly available as a result of legitimate public disclosure or as a result of court ordered disclosure.

Adverse Actions

Section 152 of the Privacy Act 2020 requires agencies to provide written notice to individuals before any "adverse action" is taken against them on the basis of personal information shared under an information sharing agreement and give those individuals 10 working days to dispute the information received.

Under the AISA, MSD may take adverse action against an individual without providing the required notice of adverse action under section 152 of the Privacy Act 2020 in the following circumstances:

(a) If the personal information shared relates to a situation where MSD has reasonable grounds to suspect that urgent intervention is required to ensure the safety of any individual from existing or potential serious harm;
(b) if, as a result of the sharing of personal information, MSD has reasonable grounds to suspect that a Serious Offence has been, or will be, committed and the Personal Information is relevant to the prevention, detection, investigation, or prosecution of that offence;
(c) If notice of adverse action may defeat the purpose of taking the action including but not limited to:
    i. any GHIC Agency's internal investigation into misconduct
    ii. seizure of assets
    iii. repayment of debts

The Parties may use their statutory powers to support these actions.

Adverse actions that MSD can be reasonably expected to take (if any) are:

(a) investigate eligibility for, or entitlement to, benefits and subsidies that are applied for or received
(b) assess whether obligations in relation to benefits and subsidies that are applied for or received have been met
(c) refuse to grant, suspend, cease, review, or reassess benefits
(d) recover debts due to the Crown.

Safeguards

MSD will comply with all of its respective policies and guidelines as well as the Solicitor General's Prosecution Guidelines (if applicable), before taking any adverse action.

MSD will:

- take all reasonable steps to confirm the accuracy of information before any action is taken;
- comply with all its relevant policies and guidelines, in addition to the Solicitor General's Prosecution Guidelines before adverse action is taken;
- ensure that it complies with its relevant legislation in regard to benefit investigation and prosecution if any adverse action is taken on a client based on information received from the GHIC;
- ensure that, when an investigation or prosecution for benefit entitlement occurs, clients are given the opportunity to comment before a decision is made on potentially prejudicial information;
- comply with all relevant provisions of their own legislation, their respective policies and guidelines and the Solicitor General's Prosecution Guidelines (if applicable), before taking any adverse action; and
- have regard to the principles of natural justice.

MSD will also take steps to ensure individuals have the opportunity to remedy any inaccuracies in the information, or misunderstandings arising from lack of context, as soon as reasonably practicable after the share occurs, having regard to all the circumstances that rendered it necessary to share the information without notifying the individual.

If Personal Information shared under the AISA forms part of the prosecution's evidence in a criminal case, the Personal Information may be disclosed to an individual in accordance with the Criminal Disclosure Act 2008. Any dispute about the provision of such Information will be managed by the courts as part of the subject matter of the prosecution.

Safeguards before providing this information will include:

1. The full name and date of birth details if available will be compared to confirm the individual's identity.
2. Where multiple individuals with the same name and date of birth exist, MSD will check biographical and other Information held about the individuals to identify them.
3. The Information will be compared for consistency with other Information held by MSD.
4. No Information will be sent via email to an individual of interest until the individual is verified as the correct person and has authorised email as the preferred method of contact.
5. Validation checks and verification of identity, including scripted questions, will form part of all contact conversations, and no Personal Information will be given to any individual until their identity is confirmed.

Accuracy and reliability of information

Data and information supplied to GHIC will be required to have passed through Quality Assurance processes for the supplying business unit. A statement will accompany every submission to SPOC confirming that:

- the Information provided to the GHIC is the most up-to-date Information that is held by MSD at the time it is provided;
- the GHIC will be notified of any constraints that may be appropriate for further use of their Information by other GHIC Agencies; and
- information shared under the AISA is of an adequate standard and quality to be used as Intelligence or the standard and quality of the Information is adequately described and caveated so that its subsequent use can reflect the standard and quality of the Information provided.

Security Provisions

MSD will follow its existing internal policies, processes and procedures for using, sharing, storing and destroying GHIC intelligence products (both electronic and physical) within the Department. Information Security as per the Protective Security Requirements (https://www.protectivesecurity.govt.nz/).

Secure Transfer of Personal Information

Documents will be sent externally by SEEMAIL and password protected, with password provided by separate channel of communication e.g. phone call or Teams message.

All information sent internally and to GHIC is classified as IN CONFIDENCE using the Microsoft Office 365 classification system. Microsoft Office 365, as configured for MSD use, will not permit a file to be sent or saved without application of a classification level.

Secure Storage of Personal Information

Information received from GHIC will be stored in Objective in a secure file folder that has been restricted to the Intelligence, Integrity and Insights Team, and SPOC.

Retention and Destruction of Information

MSD will comply with its Information Retention and Disposal Standard and the requirements of the MSD Disposal Authority under the Archives Act 2005.

Staff Obligations

MSD will ensure that their staff and contractors who have access to Information covered by the AISA are subject to contractual obligations which require compliance with MSD's Information Security policies and prohibit:

- Unauthorised access to, or use of, Personal Information which is the subject of the AISA; and
- Unauthorised disclosure of Personal Information covered by the AISA.

Code of Conduct

The MSD Code of Conduct requires staff to "work with honesty, integrity and respect", and failure to comply with its provisions can result in disciplinary action which can include termination of employment.

In particular it is considered unacceptable under any circumstances for an MSD staff member to deliberately share client details or circumstances with any unauthorised person, and if they were to do that the staff member would be investigated to determine whether serious misconduct has occurred, may be dismissed, and the matter may also be referred to the Police. MSD has a Zero Tolerance approach to any staff behaviour that impacts the integrity of the benefits system.

Acceptable Use of Technology Policy

This policy requires staff and contractors to only use approved technology, only share Ministry and client information where explicitly authorised, and take steps to keep themselves and MSD technology safe from mailicious attack. A number of other requirements are outlined in the policy.MSD staff are also subject to the Public Service Commission Standards of Integrity and Conduct.[2] These standards include obligations to:

- Keep all MSD information secure and comply with MSD's privacy and security policies
- Only access client information for legitimate work purposes
- Not access or process staff member's own records or those of friends or relatives without proper authorisation
- Not carry out or permit fraudulent activities in respect of MSD information
- Comply with all relevant information statutes including the Privacy Act 2020, the Official Information 1982, and the Public Records Act 2005.

Requests for access to and correction of Personal Information

MSD will be responsible for managing and responding to requests for access to and correction of Personal Information under Information Privacy Principles 6 and 7 of the Privacy Act 2020 as appropriate in the circumstances. This includes managing requests for Personal Information that have been provided to the GHIC and for consulting with the GHIC about their responses to those requests.

Access and correction requests are managed by the SPOC Manager and SPOC (for requests that relate to information held by the SPOC specifically in connection with the GHIC) in conjunction with the Centralised Processing Unit (where information is requested that is held by MSD in connection with its normal functions and activities).

Requests are made by individuals to the 0800 number, in person or by post to a branch office of MSD, or to the privacyoffice@msd.govt.nz inbox.

---

[2] A guide on integrity and conduct - Te Kawa Mataaho Public Service Commission

Where corrections are made to information MSD holds, the agency must ensure recipient agencies (e.g., the GHIC, and any GHIC agencies MSD is aware of that the information has been shared with) is also notified of the correction.

Privacy and Security Breaches

Assistance Statement

MSD will provide any reasonable assistance that is necessary in the circumstances to allow the Privacy Commissioner or an individual who wishes to make a complaint about an interference with privacy to determine against which GHIC Agency or the GHIC the complaint should be made.

Once that determination has been made, MSD or the GHIC's internal complaints handling procedures will apply. The internal complaints handling procedure provides for:

- The acknowledgment of the receipt of a complaint;
- The provision of information about any internal and external complaints procedures;
- The investigation of complaints;
- Reporting the results of the investigation and any actions that will be taken as a result to the complainant; and
- Providing the complainant with information about their right to complain to the Privacy Commissioner.

MSD's nominated person responsible for receiving complaints about any interference with privacy connected with the operation of the AISA is the MSD Privacy Officer. The Privacy Officer will then liaise with the appropriate internal stakeholders in order to resolve the issue.

Security Breaches

If MSD or the GHIC has reasonable cause to believe that any breach of any security provisions in or referred to in the AISA has occurred or may occur, they may undertake investigations in relation to that actual or suspected breach as deemed necessary. MSD shall ensure that reasonable assistance is provided to the investigating party in connection with all inspections and investigations. The investigating party will ensure that the other GHIC Agencies and the GHIC Manager are kept informed of any developments.

MSD may suspend its participation in the AISA to allow time for a security breach to be remedied.

Privacy Breaches

MSD will be responsible for the investigation of privacy breaches, taking account of the Privacy Commissioner's privacy breach guidelines and the obligations of the agency to report notifiable privacy breaches under Part 6 of the Privacy Act 2020.

Where Personal Information is found to have been inappropriately accessed or disclosed, MSD's internal investigation processes will be applied.

Official Information Act 1982

Any requests under the Official Information Act 1982 received by MSD in relation to the GHIC will be consulted with the GHIC, and vice versa.

Complaints

Individuals can make a complaint to MSD by way of a telephone call to one of the phone numbers set out on the MSD website[3], by post to an MSD service centre or by an email to privacyofficer@msd.govt.nz where the complaint relates to a potential breach of the Privacy Act or other misuse of MSD information.

Complaints received by email to the Privacy Officer email inbox, which is both an internal and external resource, are logged by a dedicated employee and resolved in accordance with policy and processes documented in the Privacy Officer Inbox Operational Guide, which sets out how to deal with privacy breach management, Privacy Act requests and other potential misuse of information.

Key Contacts

SPOC and Departmental Representative: Out of Scope, Principal Advisor, System Performance, Out of Scope

Protocol Review Process and Timings

This Operational Protocol will be reviewed annually by the MSD Representative, in conjunction with relevant internal stakeholders and the GHIC Manager. Any update or variation to the Operational Protocol that has more than minor, non-privacy-affecting implications will be consulted with the Privacy Commissioner before it is agreed and signed by the Chief Executive or their delegate.

Police as Lead Agency shall conduct a review biennially to check that sharing of information is being done compliantly with the AISA and the Operational Protocol. The review will specifically ensure the safeguards in the AISA are operating as intended, that they remain sufficient to protect the privacy of individuals and to ascertain whether any issues have arisen in practice that need to be resolved.

A joint review of the Operational Protocol may be undertaken whenever any GHIC Agency believes that such a review is necessary.

The GHIC Agencies and the GHIC shall cooperate with each other in any review and will take all reasonable actions to make the required resources available.

[3] Phone us - Work and Income

Requests for information (RFIs)

This page provides information on requests for information (RFIs) for Integrity Intervention Centre (IIC) staff.

On this Page:

Overview

This workstream is not a data match but a request for MSD to provide client information to three government agencies. These agencies are:

The Department of Internal Affairs - Citizenship Office (DIA)
New Zealand Police (NZ Police)
Inland Revenue (IR)

Please note the information for IR is presented in a separate section below due to a difference in the consent requirements for IR information.

IIC RFI process for DIA and NZ Police

IIC has 20 working days to respond to DIA and NZ Police requests. This work will come through S2P as a task.

MSD has agreed upon standardised questions with DIA and NZ Police.

DIA Citizenship Office

One of the standard requirements to grant New Zealand citizenship is that the applicant is of good character. Information provided by government agencies can be used by DIA to determine whether an applicant can meet this requirement.

The DIA requests are generally focused on debt-related matters.

The two main ways information can be requested are through:

a written request for the information to be released – emailed requests are acceptable
a “Consent for Release of Information” form

A signed statutory declaration can also be completed.

DIA will ask four questions for innocent debt and 14 questions for Doubtful, Deliberate and Fraudulent debts.

NZ Police

Similar to DIA, NZ Police also have a good character requirement that must be met by new recruits looking to serve the public as Police Officers.

The questions are templated and focussed on payments they have received/are receiving, debts established and repayment of these, and any investigations by MSD.

NZ Police will attach the "Consent for Release of Information" form.

NZ Police will ask four questions. The Integrity Intervention Officer (IIO) checks all MSD systems to form a general view of the client's relationship with MSD.

The Responses

The templates are saved in a folder that is accessible for staff who have been trained in RFI work.

DIA and NZ Police are filed together; requests are saved by year and alphabetically by the applicants surname.

Responses are saved first as a Word Doc, then saved as a PDF copy. MSD only send a PDF copy of our response, and this must be attached to the original request email.

IIC RFI process for IR

IIC has 20 working days to respond to requests. This work will come through S2P as a task and will be in relation to matters concerning Working for Families (WFF) payments paid by IR.

Generally, the information requested will be focused on:

debt related matters
partners
children
whether there has been an investigation by MSD
overseas travel

It is important to note that IR do not include an authority form completed or signed by the client. It is the IR investigation team that request information from MSD under the Tax Administration Act 1994 [https://www.legislation.govt.nz/act/public/1994/0166/latest/DLM348343.html] .

The Ministry is obligated to provide information to IR. Section 17B of the Tax Administration Act supersedes the Privacy Act 2020 enabling IR to obtain information relevant for their investigations without requiring the client's permission.

In order to gather information about the client for their investigation, IR will ask a series of questions. The questions will vary and may be different for each request they make.

Where a request from IR appears to be out of scope in terms of the information we would usually provide, we can seek guidance from the Integrity and Debt Information and Advice Team Out of Scope or from the Privacy Team Out of Scope at National Office.

RFI's from IR in relation to Child Support are completed by the Central Processing Unit (CPU).

The Responses

IR has a separate folder saved by year and client's surname.

Responses are saved first as a Word Doc, then saved as a PDF copy. MSD only send a PDF copy of our response, and this must be attached to the original request email.

Requests from other agencies

Occasionally you might receive requests from other government or crown agencies e.g. Ministry of Defence or Department of Corrections. IIC cannot provide information to an agency if there is no mutual agreement in place to do so.

It is possible that another part of the Ministry can respond to these requests if they have an existing agreement. For example, the Department of Corrections requests are dealt with by the Central Processing Unit, therefore you will need to forward that request to the CPU group email address Out of Scope .

A list of the RFI's that CPU complete can be found on Doogle in their knowledge base [https://doogle.ssi.govt.nz/business-groups/helping-clients/service-delivery/centralised-services/centralised-processing-unit-cpu-/knowledgebase.html] .

If you are unsure of where to forward an RFI that is from another agency, please talk to a Capability Developer or Service Manager for advice.

Release of information provided to agencies

There may be times where the agencies will advise that a client we have provided information for has requested to see the details that we have supplied. We have in the past, received these notifications from DIA, where they have declined to grant an application for NZ Citizenship based on the client not meeting the good character requirement.

This information is requested under the Privacy Act 2020 and is usually released to the client as they do have a right to ask for their own personal information. This means that the name of the IIO who completed the RFI in question, will also be released to the client.

If you receive a Privacy Act request, you will need to send this to your Service Manager who will follow up with the Privacy Team. Depending on the request, they will either confirm information can or cannot be released, what information if any needs to be redacted, or they will advise that they will provide the response to the client on our behalf.

If there are any specific concerns regarding any contact from an agency advising the release of information that we have provided for an RFI, please speak to a Service Manager, who will reach out to the Privacy Team for advice if necessary.

Content owner: Client Service Integrity **Last updated:** 03 September 2025

Information Group
Te Rōpū Whakamōhiohio

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Information Sharing

CPU Desktop Companion

May 2024

The purpose of this document

This Desktop Companion is targeted to our processors in the Central Processing Unit (CPU). It provides a general overview of what information sharing is, and our roles and responsibilities as the holding agency when we share information.

This companion focusses on the types of requests the CPU handle in their work, specifically, requests for information between government agencies. It covers the following types of requests:

- Information Privacy Principle 11, Privacy Act 2020, section 22
- Memorandums of Understanding
- Statutory Demands.

Our aim is that this Desktop Companion will sit alongside all the current CPU Learner's Guides and can be used to help process any requests for information received from other agencies, organisations, or companies.

What it does not cover

This guide does not cover all types of information sharing. Specifically, when people request their own information (Privacy Act Requests) or when people request information about other people (Official Information Act Requests).

Where to go to for more information

If you would like any more information about information sharing, or help with any type of information request, the Information Group are happy to help. Please contact us at privacyofficer@msd.govt.nz

Contents

Please follow the links below to the corresponding sections of this guide.

Information Sharing

What is 'Information Sharing'?

The Ministry of Social Development - Manatū Whakahiato Ora (MSD) interacts with over one million people each year and holds a vast amount of both personal and official information. MSD does not 'own' this information but is its trusted 'steward' and should treat information as a Taonga (treasure), to be valued and used responsibly. As stewards we can usethe Taonga we hold to improve outcomes for the individuals, whānau, and communities we serve.

Information sharing is when we share the information we hold about an identifiable individual with another agency, usually for a purpose unrelated to the reason for which it was originally collected (e.g., MSD collected a client's contact details for a job seeker application, and Police are now requesting those contact details to locate the client for an active investigation).

MSD is one of the largest sharers of information with other public service agencies, both supplying and collecting information. There are multiple, legal information sharing mechanisms that agencies can use to define what type of information can be shared, and to share that information.

Acting in good faith and cooperating with other agencies is important for the delivery of excellent, joined-up services to the people of Aotearoa - New Zealand. However, when we share information, we must make sure that we share only what the relevant sharing mechanism allows, so the public can trust that what we do is legal, responsible, and respectful.

Unless governed by a specific legal authority, **all** information sharing must comply with the Privacy Act 2020. Sometimes, for reasons in the public interest, agencies will want to share personal information in a way that would otherwise be a breach of the Information Privacy Principles (IPPs) of the Privacy Act. In those situations, an Approved Information Sharing Agreement (AISA) is required. An AISA is a formal agreement under the Privacy Act that allows agencies to agree to override specified IPPs to support the delivery of public services.

What are our responsibilities when we share information?

As the agency holding the information, MSD has a responsibility for its care and correct use. Sharing the information we hold is the *exception, not the rule* - we can only share information when the law allows us to, and it's on us if we get it wrong.

The law can either:

1. **make** us share information with another agency (i.e., a statutory demand for information under s17B of the Tax Administration Act 1994), or

2. allow us to share information if we **volunteer** to (i.e., a request for information under one of the grounds specified in s22 IPP11 of the Privacy Act 2020).

In either case, we must be satisfied that the disclosure meets the relevant statutory test for disclosure and if we do not have sufficient information to make this assessment, we should request further information from the requester.

This Desktop Companion focusses on case-by-case mandatory or voluntary requests to MSD for information relating to either an individual, whānau, or small number of individuals. Sometimes public service agencies bulk share information or set up a way to routinely share information. If you receive any requests for the bulk sharing of information, please contact the Information Group at privacyofficer@msd.govt.nz

What is a Request for Information?

An RFI is a one-off request for personal information, made to MSD by another public service agency[1]. Each time we get an RFI, it is important that we assess it to make sure we are legally allowed to share the information that's been requested by assessing the request against the relevant statutory criteria.

Generally, except in instances where there are legitimate imminent concerns for the life and safety of the public or an individual, all RFIs must be in writing, and clearly state the legal authority for the request. It is important that we record both the RFI and our response to the request, so we can later refer to them if necessary.

It is important that our response to the RFI does not exceed or provide any information that's over and above what the RFI is asking for, or what the legal authority allows us to share.

A requesting agency can use an RFI to:

1. *request* the holding agency use its legal discretion to *voluntarily* disclose the information, or
2. *demand* the information from the holding agency under a specific legal authority.

The most common types of RFIs are:

- In reliance on one of the grounds specified in Information Privacy Principle 11 of the Privacy Act 2020 (IPP 11 RFI)
- Memorandum of Understanding (MoU)

[1] A list of all public service agencies are set out in Schedule 2 of the Public Service Act 2020 (Public Service Act 2020 No 40 (as at 01 March 2024), Public Act Schedule 2 Public service agencies – New Zealand Legislation)

- Statutory Demands.

As the holding agency, we have different responsibilities when processing different types of RFIs (see following page).

Type of RFI	Our Responsibilities	Examples
Request that we *voluntarily* disclose information under one of the grounds under IPP11 of the Privacy Act 2020 You may also see a request for information using the client's consent, this could also be a request under IPP6 of the Privacy Act 2020	Assess the RFI to see if it contains enough information to allow us to form a **reasonable belief** that the information requested is required for the reason the requesting agency cites (i.e., one of the IPP 11 disclosure exceptions in the Privacy Act 2020): • if we can form the reasonable belief that the information is required for the reason cited, release the information, **OR** • if we can't form a reasonable belief that the information is required for the reason cited, refine or refuse the request.	• Police requesting the address of a person suspected of arson and they have been unable to locate the person's address themselves - ***IPP 11*** • Corrections requesting contact details of a person who has breached their bail conditions and they have been unable to locate them – ***IPP 11*** • Client has applied for legal aid. The client's lawyer has been unable to contact the client to confirm the client's financial situation and has requested benefit details from MSD – ***IPP 6***
Request that we disclose information under a Memorandum of Understanding (MOU)	Assess the request to make sure it complies with the terms of the Memorandum of Understanding it is requested under: • if it complies, release the information, **OR** • if it doesn't, refine or refuse the request.	• Memorandum of Understanding between MSD and IRD for Child Support and Domestic Maintenance. • Memorandum of Understanding between MSD and IRD for the Supply of Information for Working for Families Tax Credits Administration.
Demand information from us under a specific legal authority (Statutory Demand)	Assess the request to make sure it complies with the terms of the legal authority it is requested under: • if it complies, release the information, **OR** • if it doesn't, refine or refuse the request.	• S66 Oranga Tamariki Act 1989 • s17B Tax Administration Act 1994 • A Production Order (s74 Search and Surveillance Act 2012)

What is an IPP 11 RFI?

Information Privacy Principle 11 of the Privacy Act 2020 helps protect individual privacy in Aotearoa by preventing the agency holding personal information from disclosing it to any other agency or person, unless an exception to Information Privacy Principle 11 (IPP 11) applies. There are multiple exceptions to IPP 11 listed in s22 of the Privacy Act 2020. To make it easy, we will call each a "**Disclosure Exception**".

Agencies often cooperate and share information under a Disclosure Exception when *necessary* and in the public interest to do so. For example, to 'maintain the law' or to 'prevent a threat' to public or individual safety. However, requests for information under IPP11 should be thought of as a last resort, not a free-for-all. The requesting agency should have exhausted sources available to them (within reason). This includes seeking the information from the individual themselves, and if that is not possible, the requesting agency should tell us why.

If a Disclosure Exception applies, an agency isn't forced to share information, but has a discretion to share it voluntarily. If a requesting agency wants a us to share information under a Disclosure Exception, the requesting agency must demonstrate to us why it thinks the Disclosure Exception applies.

If we can form a *reasonable belief* from those reasons that the Disclosure Exception does apply, we can voluntarily share the information with the requesting agency. If we can't form the reasonable belief that the Disclosure Exception applies, there is no legal basis under the Privacy Act 2020 for the information share, and the request must be refused if the request cannot be further refined.

An IPP 11 RFI is a requesting agency saying to us, "*we think you have information we need to perform our legislative function and we are requesting that information under a Disclosure Exception of the Privacy Act*".

As the holding agency, we are legally required to form a *reasonable belief* that we can release the information for the reason the requesting agency is telling us (e.g., 'maintenance of the law') before we can release the information. To form a *reasonable belief*, we need to assess the request to decide for ourselves whether *we* think we can voluntarily release the information.

IPP 11 RFIs can be tricky – there are multiple Disclosure Exceptions, and we get requests from multiple public service agencies. However, once you understand how they work, the same methods of assessment can be used against any IPP 11 requests for information.

IPP 11 Request for Information Decision tree

Please see the **Decision Tree (Appendix A)**. The decision guide aims to be a visual process guide for any IPP 11 RFI, regardless of which Disclosure Exception is used. Every IPP 11 disclosure exception relies on 'forming a belief, on 'reasonable grounds'. This decision tree aims to guide you in your assessments to forming that belief.

It demonstrates the different levels of assessment required for the different levels of sensitivity of personal information being requested, which will guide you through the process of assessing when a request is reasonable and the disclosure of the personal information to the requesting agency is justified under Principle 11 of the Privacy Act 2020.

The decision tree was designed using terms found in this guide, so if you hit a bump working through the decision tree to process an IPP 11 RFI, there is guidance below explaining the process in detail. There is also guidance explaining how two of the most common Disclosure Exceptions work, and what to look for when processing those types of RFIs.

What do I look for when processing an IPP 11 RFI?

Regardless of which Disclosure Exception the requesting agency cites, one thing about processing an IPP 11 RFI always remains the same: MSD can only share information if MSD *"believes on reasonable grounds"* that a Disclosure Exception applies.

What are reasonable grounds? How do I form a reasonable belief?

Put simply, with the information you have been provided and considering the request from an objective standpoint, can you clearly see why the information being requested is needed by the requesting agency? And without that information their 'purpose' would fail?

For example:

- **Police** requesting appointment times for a client subject to an arrest warrant for a serious assault. Police have been unable to locate the client and want to intercept them away from other individuals. *They are using IPP 11(1)(e)(i) or (iv).*
- **Corrections** requesting contact, relationship, and benefit information of a client to ensure accurate records, bail condition compliance, and the client is receiving the proper cross-agency support. *They are using IPP 11(1)(e)(i) or (iv), but could also use IPP11(1)(a) or (c).*

- **MBIE** (which includes Tenancy Services) requesting client contact information in relation to an investigation against a landlord. To prosecute the landlord, they need the statements of our clients who lived there, and money MSD may have paid them. *They are using IPP 11(1)(e)(i) or (iv).*

In all those examples, if you can see how the type or amount of information being requested by those agencies is needed for them to perform their legislative function (e.g. investigating or prosecuting offences), then you have that *belief* on *reasonable grounds* that you can disclose the information under the disclosure exceptions used in the request.

To form a 'reasonable belief' when processing a request:

1. Assess the type and amount of information being requested considering the 'sensitivity' of the information.
2. Consider the steps taken by the requesting agency demonstrating the need for requesting the information from MSD (as opposed to from the person directly or using other more appropriate methods).
3. Using the information gathered from the above two steps, you can see why the requesting agency needs the information to perform their function (i.e., there is a reasonable basis for that belief).

The requesting agency must give usenough information that demonstrates why they think the Disclosure Exception applies. The processor can assess the request to see if they also think the Disclosure Exception applies. This means the requesting agency needs to provide the holding agency with sufficient background information, detail, or context to enable them to form a reasonable belief that the Disclosure Exception applies. We don't need detailed, confidential, or operational information, but we can't form a reasonable belief that the information being requested is necessary from information that is generalised and without detail.

If in doubt, ask yourself (or test your reasoning with a colleague):

- Can I explain why I believe the Disclosure Exception applies?
- Do I have the evidence to show that that my belief is reasonable?
    - I understand the information being requested and the sensitivity of that information.
    - I understand why the agency is requesting the information.
    - I can explain how the requested agency has demonstrated that they need the information (i.e., adequate detail in the RFI enabling me to form that reasonable belief that the Disclosure Exception applies)?

Sensitive Information

The more 'sensitive' the information, the greater the chance of harm to the individual if the information is improperly disclosed. Because of this, as the sensitivity of the requested information increases, so does the holding agency's disclosure risk.

To balance the risk, we need to make sure proper assessment is carried out over RFIs requesting sensitive information. The greater the sensitivity, the more robust the assessment. The more sensitive the information is, the more information the requesting agency should provide in the request, detailing why they need that type of information.

What type of personal information is considered 'sensitive' personal information is subjective, but health and financial information will likely always be considered sensitive. We have created an **Information Sensitivity Table (Appendix B)** to help you identify what level of sensitivity the requested information is likely to be.

When an agency requests information that is medium or high on the information sensitivity table, we require *context* from the requesting agency to be able to form a reasonable belief that *this* type of information is required.

For example:

- **The Police** are investigating a client as they are a suspect in a shoplifting incident. Police have requested contact details of the client from MSD as they have been unable to locate the client themselves. If the Police provided those details in the RFI, *it would be enough information* to enable a processor to form the required reasonable belief for MSD to release the information.
  - This is because the information is low on the information sensitivity table, and
  - MSD has been told why it's needed – we know from the reasons provided that without these details, the Police would not be able to locate the client, prejudicing their investigation into the shoplifting event.
- In this case, releasing the requested information to the Police would be justified under the Privacy Act 2020 section 22, IPP 11 (1)(e)(i).

BUT

- If the Police were also requesting the client's health or financial information with the same reasoning (to locate the client because of a shoplifting event), *there would not* be enough detail provided to form a reasonable belief for MSD to release the information.
  - This is because the information of high sensitivity (health or financial information).

- It isn't clear why that information is necessary to locate the client. To be able to release information of high sensitivity in this circumstance, we would require additional information from the requesting agency.

Another example:

- If **the Police** had instead told us in the RFI that the client is a suspect for shoplifting and serious Facebook fraud, we may be able to form a reasonable belief that the sensitive financial information being requested is necessary for the maintenance of the law.
- If the Police were requesting the client's benefit details and told us that it was to determine how the client had been supporting themself during the time of the suspected fraud (i.e., if their income was from a legitimate source).
  - That information would have the required detail to allow us to form a reasonable belief that high sensitivity information is required to help the Police maintain the law
  - We know that the Police need the client's financials for their fraud investigation, and why.

What is the 'maintenance of the law' disclosure exception?

Also known as the 'maintenance of the law' exception, IPP 11(1)(e)(i) allows a holding agency to voluntarily release information if it **reasonably believes** that the, 'disclosure of the information is necessary to avoid prejudice to the maintenance of the law by any public service agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences'.

IPP 11(1)(e)(i) doesn't allow a **requesting agency** to say, 'you must provide us with this information so we can maintain the law', it allows the **holding agency** to say, 'explain to me why not giving you this information would stop you from maintaining the law':

- As the agency holding the information, it's on us if we release information we're not supposed to – not the requesting agency. It's our risk, so we need to make sure we have everything we need from the requesting agency to legally release the information.

The requesting agency must provide reasons why it thinks IPP 11(1)(e)(i) applies, so that the holding agency can assess whether the request is sound:

- If the information we need to form that reasonable belief isn't provided, we must go back to the requesting agency to either refine or refuse the request.

- Our records must show that we had adequate information to be able to form a reasonable belief that IPP 11(1)(e)(i) applies.

What do I look for when processing a 'maintenance of the law' RFI?

To be able to process the RFI and release the information, the processor must be able to form **a reasonable belief** that the requested information is **necessary** for the **maintenance of the law** by a **Public Service agency**[2].

Necessary

To be 'necessary' the requested information must be needed or required in the circumstances, not just desirable or convenient to have.

Maintenance of the law by a Public Service agency

Maintenance of the law in this context relates to law enforcement action by a Public Service Agency[3], including the prevention, detection, investigation, prosecution, and punishment of offences. This exception does not apply to agencies seeking to uphold lawfulness in a general sense, it relates specifically to public service agencies which have a law enforcement function.

The Police are widely known for their law enforcement function in respect of criminal offending, but other public service agencies may also have a law enforcement function in respect of the legislation which they are responsible for administering (i.e. MSD in relation to benefit fraud, IR in relation to tax fraud/evasion, MBIE in relation to offences under the Residential Tenancies Act 1989 and Corrections in respect of the enforcement of sentences which have been imposed).

If in doubt, ask yourself:

- Is the requesting agency a public service agency which has a law enforcement function?
- Has the requesting agency provided reasons why they think *not* providing the requested information would hinder, or be detrimental to, its maintenance of the law?

[2] For further reading: Office of the Privacy Commissioner | Releasing personal information to Police and law enforcement agencies

[3] A public sector agency means an agency that is a Minister, a Parliamentary Under-Secretary, a department, an organisation, or a local authority; and includes any agency that is an unincorporated body (being a board, council, committee, or other body)— (i) that is established for the purpose of assisting or advising, or performing functions connected with, any public sector agency within the meaning of paragraph (a); and (ii) that is established in accordance with the provisions of any enactment or by any such public sector agency

- Has the requesting agency provided reasons why they think the requested information is necessary to help maintain the law?

For example:

MSD receive an **IPP 11(1)(e)(i) RFI** from the **Police**, advising they have a warrant to arrest a client on an arson charge, but cannot locate the client. The address they hold in their system is the address that was burned down in the arson, and the client's family have not assisted with locating the client. Police have requested MSD provide the client's address, contact numbers, and any future appointments with MSD, so they can locate and arrest the client for arson. Can MSD release the requested information to the Police?

Ask yourself:

Do I have a **reasonable belief** that the requested information is **necessary** for the Police's **maintenance of the law**?

The Police have told us that they've tried to locate the client by checking the client's address on their system and conducting checks with the client's family. These checks have not resulted in locating the client. This is enough information to show us why the requested information is **necessary** to locate the client.

From the information provided by the Police, MSD can infer that not providing the client's address, contact number or future MSD appointments, would mean Police could not locate and arrest the client for arson – hindering the Police's **maintenance of the law**.

The Police have told us why the requested information is necessary, and how it will help the Police maintain the law. This is enough information to enable MSD to form a **reasonable belief** that the information requested is necessary for the maintenance of the law. MSD can release the requested information to Police.

For example:

MSD receive an **IPP 11(1)(e)(i) RFI** from **Corrections** advising they are trying to locate a client who has breached bail by not residing at the bail address for two months. Corrections have stated they have exhausted all avenues to locate the client and need updated contact information, otherwise they will have to apply to the Court for a warrant to arrest the client. Corrections have requested the client's address, contact numbers, and email address so the client can be located, and their sentence managed. Can MSD release the requested information to Corrections?

Ask yourself:

Do I have a **reasonable belief** that the requested information is **necessary** for Corrections' **maintenance of the law**?

Corrections have told us they've exhausted all their own avenues trying to locate the client, and that they need to locate the client to manage their sentence, or they will have to apply for a warrant to arrest the client. This is enough information to show us why the requested information is **necessary** to locate the client.

From the information provided by Corrections, MSD can infer that not providing the client's address, contact numbers and email address, would mean Corrections could not locate the client and manage their sentence – hindering Corrections' **maintenance of the law**.

Corrections have told us why the requested information is necessary, and how it will help Corrections maintain the law. This is enough information to enable MSD to form a **reasonable belief** that the information requested is necessary for the maintenance of the law. MSD can release the requested information to Corrections.

What is the 'serious threat to safety' disclosure exception?

Also known as the 'threat to safety' exception, IPP 11(1)(f)(i) and (ii) allows an agency to disclose information if it reasonably believes the '... information [is] necessary to prevent or lessen a serious threat to public health or safety, or the life or health of the individual concerned or another individual'.

This is an important Disclosure Exception that allows an agency to release personal information to prevent or lessen a serious threat to public health or safety, or the life or health of an individual. The requesting agency must be an agency that is able to do something to prevent or lessen the serious threat (i.e., the Police).

The requesting agency **must** provide reasons why it thinks IPP 11(f)(i) or (ii) apply, so that the holding agency can **assess** whether the disclosure of the requested information is permitted:

- if the information we need to form that reasonable belief isn't provided, we must go back to the requesting agency to either refine or refuse the request.
- our records must show that we had adequate information to be able to form a reasonable belief.

What do I look for when processing a 'serious threat to safety' RFI?

To be able to process the RFI and release the information, the processor **must** be able to form a **reasonable belief** that the requested information is **necessary** to prevent or lessen a **serious threat** to public health or safety, or to the life or health of an individual.

Necessary

To be 'necessary' the requested information doesn't have to be essential, or indispensable, in order to help the requesting agency prevent or lessen a serious threat, but it must be needed or required in the circumstances, not just desirable or convenient to have.

Serious threat

A 'serious threat' is a threat that, if eventuated, could result in serious, harmful consequences to public health or safety, or to the life or health of an individual. When processing a request, there are three factors to think about to help determine if the threat is serious:

1. What is the likelihood of the threat being realised?

- How likely is it that the threat will happen?

2. How severe are the consequences if the threat is realised?
   - What are the consequences to public health or safety, or individual health or safety, if the threat is realised? How bad are they?
3. When may the threat be realised?
   - How soon might the threat occur?

Each threat should be assessed in context, and all relevant circumstances should be considered when assessing the threat. All three factors **do not** have to be present for the threat to be serious:

- A threat that, if realised, has severe consequences for the individual concerned may be considered a serious threat even if we are unsure of its likelihood or when it will occur.
- A threat that has serious consequences and a high likelihood of occurring is likely to be a serious threat, even if we are unsure of how immediate the threat is.
- A threat to a tamaiti will more readily meet the 'serious threat' threshold because tamariki are vulnerable and have limited capacity to act for themselves.

For example:

MSD receive an **IPP 11 (1)(f)(ii)** from **Police**. The Police are trying to locate a client to conduct a welfare check because the client threatened self-harm when MSD declined hardship assistance (MSD reported this to the Police). The Police have advised they have been unable to contact the client and urgently need the client's contact details to check their welfare.

Ask yourself:

1. Do I have a **reasonable belief** that there is a **serious threat** to the life or health of an individual?
2. Is the release of the requested information **necessary** to prevent or lessen the serious threat?
3. Is the release to an agency who can do something to prevent or lessen the serious threat?

The Police have told us that the client reported they would self-harm after being declined hardship assistance. This is enough information to enable us to form a **reasonable belief** that there is a **serious threat** to the life or health of an individual – we know that if realised, the consequences of the threat are very severe and that given the threat was a reaction to being declined hardship assistance, we know it is likely that the threat may occur soon.

The Police have also told us they have been unable to contact the client to conduct a welfare check. This is enough information to show us why the requested information is **necessary** – it is required in the circumstances to locate the client to prevent or lessen the serious threat of self-harm.

We also know that Police are the proper agency to disclose this information to, as they are the agency tasked with conducting welfare checks for any reports of concern. MSD can release the requested information to the Police as the information is necessary to prevent or lessen a serious threat to the life or health of an individual and the Police is an appropriate agency for responding to this threat.

For example:

MSD receive an **IPP 11 (1)(f)(ii)** from **Police**. The Police are investigating a missing person report and have stated there are real safety concerns for a client: the client is elderly, has dementia, and has not been seen for over 24 hours. Police have urgently requested the client's bank account details from MSD, so they can issue a Production Order to the client's bank to help locate the client and make sure they are safe.

Ask yourself:

1. Do I have a **reasonable belief** that there is a **serious threat** to the life or health of an individual?
2. Is the release of the requested information **necessary** to prevent or lessen the serious threat?
3. Is the release to an agency who can do something to prevent or lessen the serious threat?

The Police have told us that the client is elderly, suffers from dementia, has been reported missing and not been seen for over 24 hours, this is enough information to enable us to form a **reasonable belief** that there is a **serious threat** to the life or health of the individual concerned. We know that if the client is not located, there may be serious consequences to the life, health, or safety of the client. We also know that the likelihood of the threat being realised is imminent (i.e., happening in real-time) as the client has not been seen for over 24 hours.

The Police have requested the client's bank account so they can get a Production Order to give to the bank to obtain further information to help locate the client (i.e., transaction history). This is enough information to show us why the requested information is **necessary** in the circumstances to prevent or lessen the threat. If MSD do not provide the requested information, the Police may not be able to get transaction history from the client's bank to help locate the client to prevent or lessen the serious threat to the client's safety.

We know that Police are the proper agency to disclose this information to as they're the agency tasked with conducting welfare checks for any reports of concern. MSD can release the requested information to the Police as the information is necessary to prevent or lessen the serious threat to the life or health of an individual.

What to do if a requesting agency has used the wrong disclosure exception?

Occasionally an agency may cite the wrong Disclosure Exception in their RFI. In most circumstances, we would send these RFIs back to the requesting agency and ask them to refine the RFI by citing the correct Disclosure Exception. We wouldn't release the information until the correct Disclosure Exception is cited (and the RFI is sound).

However, if the circumstances mean that not providing the information would have a greater negative impact to the situation that generated the RFI, we may be justified in releasing the requested information under another Disclosure Exception. This should **only** happen in **urgent** circumstances, and if we release, we need to **clearly** cite for our records that we are releasing under that Disclosure Exception, and not the one cited by the requesting agency.

For example:

Police are trying to locate a client to conduct a welfare check, as the client threatened self-harm when they were declined for hardship assistance from MSD. MSD reported this to the Police. The Police have advised they have been unable to contact the client and need the client's contact details urgently to check on the client's welfare.

Police have stated in their RFI that the information is requested under **IPP 11(1)(e)(ii)** - for the enforcement of a law that proposes a pecuniary penalty. We know that the information provided in the RFI does not meet the criteria for release under that Disclosure Exception but would be meet the criteria for release under Disclosure Exception **IPP 11(1)(f)(ii)** - to prevent or lessen serious threat to safety to life of individual.

In these **urgent** circumstances, asking the Police to refine their RFI to site the correct Disclosure Exception is justified, but may worsen the threat to the safety of an individual. The information could instead be released to Police with a statement noting: 'this information has been released under the Privacy Act 2020 - Section 22, Principle 11(1)(f) as it has been deemed necessary to prevent or lessen a serious threat to the life or health of the individual concerned or another individual.'

What is an RFI under a Memorandum of Understanding?

A Memorandum of Understanding (MoU) is a formal agreement that records how two or more agencies will share personal information to support delivery of specific services or outcomes. It is a statement of the participant agencies' shared understanding of the proposed information share. Simply put, it's saying 'this is how we will work together to manage the information we share with each other'. It defines the roles and responsibilities of each participating agency, including what to with the information when things go right, and what we will do if it goes wrong.

To be clear, an MoU does not provide a legal authority to share information or require MSD to provide any information where it is not satisfied that there is a legal authority to do so, MOUs essentially provide for agreed operational rules that are to govern the sharing of information based on a pre-existing legal authority under the Privacy Act 2020, an AISA or other legal authority (i.e., the Tax Administration Act 1994).

An MoU is beneficial because it clarifies expectations in respect of the lawful authority for sharing information making regular sharing where similar conditions exist more efficient between agencies. It's a formal way of recording, in writing, the willingness of the parties to work together to achieve the outcomes of each party.

MoUs provide:

- Certainty about the purpose of sharing personal information.
- Recognition of the agencies' roles and obligations.
- Safeguards and technical descriptions of how the information will be shared.
- Remedies if things go wrong because of the sharing.

MSD operates many MoUs with different agencies, including:

- Inland Revenue - Te Tari Taake (Child Support, Child Support Pass On and WFF/benefit payments).
- Ministry of Education - Te Tāhuhu o te Mātauranga (locating tamariki who aren't enrolled/attending school).
- Corrections - Te Ara Poutama
- Police - Nga Pirihimana o Aotearoa (to monitor Child Sex Offenders CSOs).

What do I look for when processing an RFI under an MoU?

An MoU sets out what type of information can be shared between participating agencies, and for what purpose. This is helpful because when processing an RFI under an MoU, the terms of the MoU provide operational 'rules' for processing the request.

If the terms of the MoU allow the requested type of information to be shared – then we can release the information. By sticking within the defined rules of what the MoU allows, we have a process to follow for each RFI – regardless of what MoU an RFI sits under.

We can release the information to the requesting agency if the RFI:

1. is from a participating agency; and
2. the information requested complies with the terms of what the MoU allows to be shared.

Most learner guides tell you what information can be shared under which MoU. However, if you get stuck processing an RFI under an MoU, it can be helpful to check the MOU itself to see what information the terms of the MoU allows to be shared. We have created a **CPU MoU Stocktake (Appendix C)** of the MoUs that the CPU are most likely to see when processing RFIs.

The CPU MoU Stocktake lists the MoUs and gives a breakdown of each MoU's:

- participating agencies
- purpose of the information exchange, and
- type of personal information that can be provided by MSD.

If you need any help processing an RFI under an MOU, please contact privacyofficer@msd.govt.nz

What is a Statutory Demand for information?

A statutory demand for information, or a demand for information under a search warrant or production order, are **mandatory** requests for information set out in statute/law. The holding agency **must** comply with the demand and provide the requested information (if held).

The holding agency is required by law to comply with demands because they operate under specific legal authorities that, in those cases, override the Privacy Act 2020. Although the Privacy Act 2020 doesn't apply to demanded information, it does apply to any information provided beyond the scope of the demand. We must be careful not to overshare, and to only provide the information allowed by the underlying legal authority.

There are different types of statutory demands, under different specific legal authorities, for different reasons.

For example:

- s17B of the Tax Administration Act 1994 gives the Commissioner of Inland Revenue a 'statutory power' to require information, or the production of documents, for purposes of administering an Inland Revenue Act.
- s66(1) of the Oranga Tamariki Act 1989 enables Oranga Tamariki and the Police to demand information that may affect or relate to the safety and wellbeing of te tamaiti or rangatahi from an agency, if the information is needed for the reasons listed in s66 (aimed at protecting the welfare of tamariki).
- Production Orders served by Police Officers.

Each specific legal authority will tell us what information can be shared and why. A search warrant or a production order will also tell us what type of information can be demanded.

What do I look for when processing a Statutory Demand?

The specific legal authority used to demand the information will set out what information can be shared and for what purpose. Like MoUs, this gives us 'defined rules' for the share. If the specific legal authority allows the requested type of information to be shared – then we can release the information. By sticking within the defined rules of what the specific legal authority allows, we have a process to follow for each statutory demand – regardless of what specific legal authority is used.

We can release the information to the requesting agency if the demand:

1. is from the correct agency, and
2. the information requested complies with the terms of what the underlying legal authority allows to be shared.

Most learner guides tell you what type of information can be requested under which specific legal authority. Often, it will be helpful to check the specific legal authority itself, to see what information it allows to be shared. We have created a **Statutory Demand Table (Appendix D)**. This table provides a breakdown of some common statutory provisions and explains what type of information can be demanded under that provision.

If you need any help processing a statutory demand, please contact privacyofficer@msd.govt.nz. There is further guidance below on statutory demands.

What about requests for information under the Oranga Tamariki Act 1989?

What should I look out for when processing a request under s66C?

Section 66C Requests ('Voluntary')

Section 66C allows us (as a Child Welfare and Protection Agency) to disclose information we hold relating to a tamaiti or rangatahi (young person), to another Child Welfare and Protection Agency or Independent Person, if we **reasonably believe** that the requested information will assist the requesting agency to carry out any of the purposes set out in s66C(a), those being:

- preventing or reducing the risk of a tamaiti or rangatahi being subject to harm, ill-treatment, abuse, neglect, or deprivation, or
- making or contributing to an assessment of risk or need in relation to a tamaiti or rangatahi, or any class of children or young persons, or
- making, contributing to, or monitoring any support plan for a tamaiti or rangatahi, where the plan relates to the activities and functions of Oranga Tamariki ("the department"), or
- preparing, implementing, or reviewing any prevention plan or strategy issued by Oranga Tamariki, or
- arranging, providing, or reviewing services facilitated by Oranga Tamariki for a tamaiti or rangatahi and their family or whanau, or
- carrying out any function in relation to family group conferences, tamariki or rangatahi in care, or other functions relating to care or protection under Part 2 of the Oranga Tamariki Act 1989.

Although requests made under section s66C of the Oranga Tamariki Act are made under a statute, they aren't statutory demand, just like IPP11 requests, they require us to form a reasonable belief that the information is required to enable the requesting agency to carry out one of the above purposes.

To be able to form a **reasonable belief** that the information requested will assist with carrying out one of the listed purposes, the requesting Child Welfare and Protection Agency or Independent Person needs to tell us:

- The type of information required.
- Why is it required.
- What will the information be used for.
- Information about any relevant timeframes (is it urgent?).

- Any contact details for the person the information is about (for the purpose of consulting).

If the requesting Child Welfare and Protection Agency or Independent Person has not provided enough information to enable us to form a **reasonable belief** that the information is required for one of the listed purposes, we will need to refine or refuse the request.

Section 66C Requests to be made on template forms

Ideally, all section 66C requests will be made using one of the following forms:

- Information-Sharing-Request-Template-Agency-to-Agency.pdf (orangatamariki.govt.nz)
- request-for-information-s66-s66c-form.pdf (orangatamariki.govt.nz)

These forms have been developed by Oranga Tamariki and cover the key information and context that MSD needs to assess to be satisfied of in responding to section 66C requests.

Provided these forms have been adequately completed, CPU may release the requested information provided it has considered whether consultation with the child or young person is practicable or appropriate (see **Obligation to Consider Consultation with Child or Young Person** below).

Section 66C Requests not made on template form

If requests are not made on the template form, we should still assess them to consider whether we can release the requested information. In those cases, assess whether the request:

1. Is the request from a child welfare and protection agency or independent person?

   This step is met if the request is from anyone from Oranga Tamariki because Oranga Tamariki is a "child welfare and protection agency".

2. Does the request relate to a child or young person or any class of children or young persons?

   There are no limits in section 66C on who the information might be about, but it must relate to a child or young person (singular or plural). This could be things like:

   - details about who works with tamariki or whānau (like schools or doctors) and why
   - details about the home environment

• descriptions about tamariki and whānau needs, aspirations, strengths, what's working well (physical or mental health, education, behaviour, and social connections)

• an outline of challenges whānau are facing (like financial pressure, housing difficulties, family violence concerns or alcohol and drug issues)

• information about who or what has helped tamariki or whānau in the past or what challenges and concerns there have been in the past for tamariki, or people around tamariki.

3. Is the information requested for any of the following purposes:
   - preventing or reducing the risk of a child or young person being subject to harm, ill-treatment, abuse, neglect, or deprivation, or
   - making or contributing to an assessment of risk or need in relation to a child or young person, or any class of children or young persons, or
   - making, contributing to, or monitoring any support plan for a child or young person, where the plan relates to the activities and functions of Oranga Tamariki, or
   - preparing, implementing, or reviewing any prevention plan or strategy issued by Oranga Tamariki, or
   - arranging, providing, or reviewing services facilitated by Oranga Tamariki for a child or young person and their family or whanau, or
   - carrying out any function in relation to family group conferences, children or young persons in care, or other functions relating to care or protection under Part 2 of the Oranga Tamariki Act.

   This step requires the requester to state which of above purposes it requires the information for.
4. Has the requester provided sufficient information for MSD to hold a reasonable belief that disclosing the information will assist the requester to carry out one or all of the purposes stated in step 2?

   This step requires MSD to be satisfied that the requested information will assist the child welfare and protection agency or Independent Person with the stated purpose (or purposes) for which it is requested. If this is not apparent from the request, CPU should request further detail from the requester.
5. Is it practicable and appropriate to inform the child or young person concerned, or their representative, about the proposed disclosure?

   See **Obligation to Consider Consultation with Child or Young Person** below.
6. If the answer to step 5 is no, the information can be released.

If the answer to step 5 is yes, then consult with the child or young person concerned or their parent/guardian prior to forming a decision on release:

Consultation requires the child or young person concerned, or their representative (any parent or guardian), to be informed of the proposed disclosure and provided with reasonable assistance to understand the proposed disclosure.

This step requires MSD to take the views of the child or young person into account but does not require MSD to obtain consent.

Obligation to Consider Consultation with Child or Young Person

- This obligation applies when MSD considers it is *practicable or appropriate* to consult with a child or young person (or their representative) who is subject to a section 66C request.
- It might not be practicable or appropriate to consult with the child or young person concerned (or their representative) if:
  - they are not developmentally able to understand
  - it might put them or someone else at risk of harm
  - it might distress or upset them, or have a negative impact on their wellbeing
  - it could get in the way of a Police investigation or prosecution
  - you need to share information quickly because the child or young person might be harmed otherwise
  - after making reasonable efforts you, or another professional, can't get in touch with them, and you still think sharing is important to protect the child or young person from harm.
- There is no obligation to consult with children or young people about sharing *other people's* information under section 66C (like a family member's criminal history)

Section 66(1) – Agencies to supply information

Section 66(1) is a statutory demand; MSD must comply with requests under s 66(1) unless the information requested is legally privileged.

There is no obligation to consult or consider consulting the child or young person, we simply disclose the information requested if satisfied that the information is not legally privileged and meets the criteria set out below.

Requests should be made on the following form:

- request-for-information-s66-s66c-form.pdf (orangatamariki.govt.nz)

However, if these requests are not made on this form, you should forward them through to the Information Group for guidance.

Glossary

Approved Information Sharing Agreement (ASIA)

A *legally binding* agreement that *outlines the conditions for sharing information between* agencies to support the delivery of public services. AISAs are authorised through an Order in Council process – they become the law. A breach of an AISA is considered *as a breach of the Privacy Act*.

AISAs can authorise information sharing even if it would otherwise breach some of the privacy principles in the Privacy Act.

Generally, any sharing under the legal authority of an AISA should be done in accordance with an MOU.

Child welfare and protection agencies:

- The Department of Corrections
- The Ministry of Health
- The Ministry of Social Development
- The Ministry of Education
- The Ministry of Justice
- The New Zealand Police
- Housing New Zealand Corporation
- Oranga Tamariki – Ministry for Children
- Every registered community housing provider (as defined in section 2(1) of the Public and Community Housing Management Act 1992)
- Every DHB
- Every school board (as defined in section 15(1) of the Vulnerable Children's Act 2014)
- Every early childhood service (as defined in section 309 of the Education Act 1989)
- Any person, body, or organisation that provides regulated services (as specified in Schedule 1 of the Vulnerable Children's Act 2014)
- Any organisation or class of organisation designated as a child welfare and protection agency by regulations made under section 447(1)(ga)(i) of the Oranga Tamariki Act.

Disclosure

The action of providing MSD *held* information to another agency, *organisation, or person* (providing the information requested).

Disclosure Exception

*This is what we have called t*he *specific* legal mechanism that allows MSD to share information with another agency when it should otherwise remain private. *For example, IPP11(1)(e)(i) is the 'disclosure exception' for maintenance of the law type requests for information.*

Good Faith

Good faith, in relation to information sharing, means that requesting agencies make their best efforts in following the requirements of a public service agency's obligations under relevant legislation (i.e., the Privacy Act 2020, Oranga Tamariki Act 1989, etc)

In regard to information sharing made under the Oranga Tamariki Act 1989, if we share information in good faith, and in line with the provisions, we are generally protected from any kind of criminal, civil or disciplinary action (as per s16 of the Oranga Tamariki Act 1989)

Holding Agency

The agency holding the requested information. For the purposes of this document, and for your work, the 'holding agency' is the Ministry of Social Development

Independent person (under the Oranga Tamariki Act 1989):

- A practitioner registered under the Health Practitioners Competence Assurance Act 2003 who provides health or disability support services
- A Children's worker (as defined in section 23(1) of the Vulnerable Children's Act 2014)
- A person or class of persons designated as an independent person by regulations made under section 447(1)(ga)(ii) of the Oranga Tamariki Act.

IPP

One of the Information Privacy Principles contained within section 22 of the Privacy Act 2020

Memorandum of Understanding (MoU)

A formal agreement that records how two or more agencies will share information to support delivery of specific services or outcomes. An MoU doesn't provide legal authority for information sharing. There needs to be an underlying legal basis to allow the information sharing (typically a disclosure exception of the Privacy Act 2020 or another piece of Legislation which allows the sharing of information).

An MoU can be considered as a statement of the participant agencies' shared understandings of their roles and responsibilities to share information for an agreed purpose at the time the MoU was signed. It's saying 'this is how we will manage the information that we share with each other'.

Necessary

Relating this to information sharing, this would be the information *required to achieve a specific purpose or goal. It implies a careful balance between the need*

to share information for a legitimate purpose (i.e. Police request information to investigate an offence), and protecting the individuals' privacy rights.

Public Sector Agencies
A broad range of organisations that serve as instruments of the Crown in respect to the Government of New Zealand. However, not all public sector agencies can request information under the Privacy Act 2020, this is usually reserved for public service agencies (and police)

Requests for information from organisations such as body corporates, local government authorities, and crown entities (which can sometimes be viewed as included in the wider public service) are responded to under the Official Information Act. If you receive a request for information from an organisation not listed here, contact the Information Group for support.

Refine
Going back to the requestor *with questions gathered from initial assessment* to seek further *clarification* and context to allow assessment.

Requesting Agency
The agency requesting the information from the Holding Agency

Reasonable Belief
An idea based on what an objective, reasonable person, with similar knowledge, experience and context would believe or do in a particular situation.

RFI
Request for Information made from another *public service* agency to MSD for information that we hold. This can be under a ground specified in Principle 11, s22 of the Privacy Act 2020 or other legislation which allows agencies to make voluntary requests for information from MSD.

Statutory Demand
A power given to agencies under Legislation they operate under to compel MSD to provide information. Not providing the requested information may be an offence against the Act that gives the agencies this power. These requests don't require an assessment like a voluntary request as the responsibility for invoking this power falls onto the requesting agency. Instead, we check to ensure the scope of the information demanded is correct (for example, legally privileged information usually isn't allowed).

Steward (Stewardship)
Stewardship is a duty of care for a resource. For MSD, this would be the information we hold about our clients.

Voluntary Request
What we have called a request made for information that MSD is not compelled to provide. Typically, *these refer to request* made under a ground specified in IPP 11 of the Privacy Act 2020, these require assessment and can be refused should MSD not *be able required to form the reasonable belief that the requested information in necessary. Just remember*, other Legislation can give agencies the ability to request, or demand, information from MSD (i.e. the Oranga Tamariki Act 1989)

Glossary of kupu Māori

Tamariki/tamaiti
Children/child

Rangatahi
young persons

Kaitiaki
a minder, custodian, keeper, or steward

Taonga
a treasure, anything that is prized. It can be applied broadly to anything considered to be of value.

Appendix A: IP 11 Requests – Public Service Agency requesting MSD held information

If the answer is 'no' to any of the steps below, please go back to the requestor and refine.

Release information only when you are satisfied with the answers to the questions below:

1 **Have they stated the 'purpose' of the request?**

Example:
- Maintenance of the Law (e)(i – iv)
- Public Health or Safety (f)

2 **Has the requesting agency identified themselves?**

Example: 'I am an investigator for...', on Official templates with signatures on the request used, or anything else that identifies who they are and their role

3 **Have they provided enough personal information for us to identify the individual subject to the request?**

Example: Police requesting the identity of a client with a particular contact number and address)

Low risk

4 **Have they identified the individual's role in the situation?**

Is the client a:
Witness? Victim? Person of interest? There must be a causal link between the individual and the reason for the request

5 **Have they clearly identified the information they're requesting?**

If so, is it:
Low risk - contact details
Medium risk - Benefit information
High risk - health information, appointment locations, etc

6 **Is there a valid need for the information being requested?**

- Are they wanting to check the accuracy of their records so they can make contact?
- Is there an offence?
- Is there an investigation?

7 **Have they stated what steps they've taken to source the information via different avenues?**

Have they:
- Accessed their own records?
- Attempted to locate
- Provided adequate reasons why this isn't an option?

Medium risk & High risk

8 **Are we confident that reason for the request aligns with the exception used in the request?**

Does the reason for the request line up with the original purpose of the request? Can you see the link?

Appendix B: Information Sensitivity Table

This is not an exhaustive list. This is a quick guide that references what kind of personal information you generally provide in your day-to-day work, and the typical sensitivity of the requested information.

Low Simple reason required from requestor as to why this is needed from MSD	Medium Reason and context required from requestor as to why this information is needed from MSD	High Reason, context and steps taken required from requestor as to why this is needed from MSD
• Name/Known Aliases • Date of birth • Known Physical Address • Known Email Address • Known Contact Numbers • Spoken Languages • Benefit Status (Yes or No)	• Client numbers • Unique Identifiers • Bank account numbers • Detailed benefit status • Gender • Staff Information • CCTV Footage • Last Contact with MSD	• Health Information • Disability Information • Mental Health Information • Information about Children • Sexual orientation • Race • Future appointments with MSD

Remember:

Risk is subjective. We have categorized personal information in the above way to show certain information doesn't require as robust assessment as others. A request for nothing more than contact information will likely always be allowed, and so does not require the kind of assessment expected for health information. This table serves as a guide to how much assessment is required for the requests you see in your work.

If you're unsure about a piece of personal information your assessing, reach out to the Privacy Officer for guidance support

Appendix C: CPU specific MoU Breakdown

Participating Agencies	MoU Name (and purpose)	Information Shared to MSD (and use)	Information Shared by MSD
Corrections ***Ara Poutama Aotearoa*** **Kāinga Ora** **Police** ***Ngā Pirihimana o Aotearoa***	Agreement for Sharing Information about Child Sex Offenders, Department of Corrections, Ministry of Social Development, Housing New Zealand Corporation and New Zealand Police *To monitor compliance by the CSO with his or her release conditions, conditions of a sentence of supervision, intensive supervision, community detention, or home detention, post detention conditions of a sentence of home detention, or conditions of an extended supervision order. Also to manage the risk that the CSO may commit further sexual offences against children, or to identify any increased risk that the CSO may breach his or her conditions or will commit further sexual offences against children and to facilitate the re-integration of the CSO into the community*	• CSO name and aliases • Gender • DOB • Address • Main reporting centre • SWN Number • Conditions from Probation Officer Education, training or employment conditions from probation office Attendance and conditions at required programmes • Re-integration conditions with family Potential risks of re-offending Changes in CSO circumstances *To monitor Child sex offenders and to make sure they comply with their release conditions*	• Any new information about CSO potentially coming into contact with a child or young person • Behaviour information; Referral or placement into employment, training or voluntary work • Benefit Status • Change of addresses • Change in accommodation • Association risk with children
Inland Revenue ***Te Tari Taake***	Memorandum of Understanding for Child Support and Domestic Maintenance between Inland Revenue and The Ministry of Social Development *To assess the minimum level of financial support payable by certain parents in respect of their children and to provide for collection and payment of child support and domestic maintenance. Support clients apply for Child support*	• SWN number • IRD number • Client personal information • Benefit information • Bank account information • Personal information of partner receiving care payments • IRD number of Partner receiving care payments • Child personal information *To record all deduction notices received from IR against the respective Liable Person's SWIFTT record. The same deduction notice shall remain in force until revoked or amended by IR regardless of the type of benefit paid. This will ensure that MSD continues to apply the deduction when the Liable Person transfers from one benefit to another.*	• SWN number • IRD number • Client personal information • Benefit information • Bank account information • Personal information of partner receiving care payments • IRD number of Partner receiving care payments • Child personal information

Inland Revenue ***Te Tari Taake***	Memorandum of Understanding for the Exchange of Information between Inland Revenue and Ministry of Social Development for Working for Families Tax Credit and Benefit Double Payment *To determine eligibility and amount of Benefits for clients as well as eligibility for Entitlement Cards and to identify those on Working for Families Tax Credits*	• IRD Number • Client Personal Information • Employer Information • Income Information • SWN Number • Benefit Information • Tax Credit Information • Client partner information • Client Partner IRD Number • Client Partner Address • Client Children Information *To enable MSD to verify the entitlement or eligibility of any Beneficiary to or for any benefit including verifying the amount of any benefit and entitlement to these benefits and to issue entitlement cards to those eligible.*	• IRD Number • Client personal information • Benefit information • SWN Number • Tax Credit Information
Inland Revenue ***Te Tari Taake***	Memorandum of Understanding between the Ministry of Social Development and the Inland Revenue Department for the Supply of Information for Working for Families Tax Credits Administration *To enable MSD to provide Beneficiary Information to Inland Revenue to facilitate the timely commencement, cessation and correct calculation of entitlements to Working for Families Tax Credits.*	• IR pay frequency • Benefit information • SWN number • Client Personal Information • IRD number • Date client arrived in NZ • Client bank account number • Weekly income information • Partner IRD number • Partner SWN • Partnership known date • Partner Benefit Information • Partner weekly income information • Partner name + DOB • Children names + DOB • Children benefit information	• IR pay frequency • Benefit information • SWN number • Client Personal Information • IRD number • Date client arrived in NZ • Client bank account number • Weekly income information • Partner IRD number • Partner SWN • Partnership known date • Partner Benefit Information • Partner weekly income information • Partner name + DOB • Children names + DOB • Children benefit information

		Use not specified	
Inland Revenue ***Te Tari Taake***	Memorandum of Understanding Relating to the sharing of information for Child Support Pass-On system testing ahead of operational use (Part 7 of the Privacy Act 2020 and Section 18E(2) of the Tax Administration Act 1994) Ministry of Social Development and Inland Revenue Department *To enable MSD to test the matching of child support payments to customer records and calculation of benefit entitlements.*	• IRD number • SWN number • Name • DOB • Phone number • Email address • Residential address • Other names • Child Support details • Transaction information • Child support Liability information *Information provided will be matched against MSD customer records and successfully matched transactions will proceed to an assessment to determine benefit entitlements including the child support payments as a source of income*	• IRD number • Child Support Start/End month
Inland Revenue ***Te Tari Taake***	Child Support Payment File Exchange *To assess eligibility, entitlement for and whether obligations have been met (including recovery of debt) in relation to benefits and subsidies.*	• IRD number • SWN number • Name • DOB • Phone number • Email address • Residential address • Other names • Child Support details • Transaction information *To assess eligibility and entitlement to benefits and subsidies with child support treated as income in the assessment.*	• IRD number • SWN number • Name • DOB • Phone Number • Email address • Residential Address • Other names
Inland Revenue	Child Support Liability Exchange	• IRD number • First name, middle name, surname	• IRD number

Te Tari Taake	*To assess eligibility, entitlement for and to assess and enforce obligations (including the recovery of debt) in relation to benefits and subsidies.*	• Date of birth • Liability month/year • Liability amount • Liability day count (for the month) • Liability type *To assess eligibility and entitlement for TAS and SpB and enforce obligations including recovering any associated debt in relation to TAS and SpB.*	
Ministry of Education ***Te Tāhuhu o te Mātauranga***	Memorandum of Understanding Between Ministry of Social Development and Ministry of Education for the purpose of sharing information to support locating children and young people either not enrolled in school or not attending school due to exclusion *To help Education fulfil its obligations under section 16 of the Education Act,* *and/or to detect, investigate and prevent offences under section 24 and* *section 29 by locating the parents/caregivers of non-locatable students.*	• Case ID (education use only) • Child's Names • DOB • Caregivers name • Caregivers address • Advisor (Education use only)	• Any known contact details of parents/caregivers of listed children

Appendix D: Statutory Demand Table

Agency	Authority	Procedures for Release
NZ Police ***Ngā Pirihimana o Aotearoa***	Production Orders under section 74 of the Search and Surveillance Act 2012 are made by an Issuing Officer on the application of an enforcement officer (usually Police). An Issuing Officer is defined as: (a) a Judge: (b) a person, such as a Justice of the Peace, Community Magistrate, Registrar, or Deputy Registrar, who is for the time being authorised to act as an issuing officer under section 108 MSD is required to comply with the Production order and release all the information requested. If they ask for it, we provide it! Not providing the information is an offence under section 174 of the Search and Surveillance Act 2012.	Client is able to be located in CMS from the Production Order (PO). The PO is free from defects and isn't missing any details e.g. states PO is for MSD, has the correct client information and the name number or stamp of the issuing officer is stated in the PO. If this is not stated correctly on the PO (i.e. is unsigned/no stamp), the PO is invalid and must be sent back to the Police to rectify. If the PO is free from defects, MSD is required to produce all the information requested in the PO before the end of the PO's duration date has ended. Police do have the option to request additional information on an ongoing basis while the PO is in force. If this is the case, MSD is still required to produce the requested information. If you come across this and are unsure, seek advice from privacyofficer@msd.govt.nz
Oranga Tamariki	Section 66(1) of the Oranga Tamariki Act 1989. MSD must provide the requested information if this relates to the care and protection of a child or conduct of proceedings under part 2 of the Oranga Tamariki Act. Requested information can include (but not be limited to) Name, DOB, address, info that clearly relates to the care and protection of a child.	**S 66(1) – Agencies to supply information** **MSD must comply with requests under s 66(1)** unless the information requested is legally privileged. There is no obligation to consult or consider consulting the child or young person concerned in respect of section 66(1) requests. Requests should be made on the following form: • request-for-information-s66-s66c-form.pdf (orangatamariki.govt.nz) If these requests are not made on this form, MSD should be satisfied that the following criteria is met: *1. The request is made by:* *a. the Chief Executive of Oranga Tamariki (or someone acting under delegated authority),* *b. a care and protection co-ordinator; or* *c. a constable* *2. The information requested relates to or affects the safety or well-being of a child or young person* *3. The request states the information is required for either of the following purposes:* *d. A determination of whether a child or young person is in need of care or protection or assistance under s 17(2) and (2A) of the Oranga Tamariki Act; or* *The purposes of any proceedings under Part 2 of the Oranga Tamariki Act (including family group conferences)*

Inland Revenue ***Te Tari Taake***	Section 17B of the Tax Administration Act 1994. IRD have broad powers under s17B to request any information to help administer or enforce an Inland Revenue Act. MSD must provide any information requested by Inland Revenue under s17B if it relates to the enforcement of an Inland Revenue Act. In practice this is broad and relates to all laws where people pay money, or receive payment of money (i.e., child support, income tax etc). If IRD ask for anything broadly relating to *who gets paid, or pays what, when* - we provide the information!	On notice in writing, MSD is required to provide any information and produce for inspection any books or documents the Commissioner believes is relevant to their investigation. IRD is required to advise their request is under section 17B of the Tax Administration Act 1994, if this isn't stated, refine the request with IRD. If section 17B is stated on the request for information, and you are able to locate the client with the information provided on the request, MSD is required to supply all of the requested information.