

5 December 2022

J A Harris
fyi-request-20919-643c5344@requests.fyi.org.nz

Dear J A Harris

Request for information

Thank you for your Official Information Act 1982 (OIA) request of 19 October 2022, in which you asked for statistics and information relating to Privacy Act requests received by Police.

My response to each of your questions can be found below.

- 1. Statistics relating to the number of principle 6 privacy act requests received by Police in the 18 months to 31 July 2022. Include the number of requests received, time to respond with the decision or information, statistics relating to the number of requests which are denied and the reasons for denying which are relied upon, statistics relating to situations where the OPC have required or advised police to release information they tried to withhold.*

Police has identified 8094 requests by individuals for their personal information (Privacy Act requests) received in the period 1 February 2021 to 31 July 2022.

While retrieving this information Police identified that some Privacy Act requests had been incorrectly logged in Police's Information Request Tool (IRT) as OIA requests. Based on those instances that have been identified this only impacted how the requests were recorded, they were still managed and responded to as Privacy Act requests.


As it would require a manual review of each of the over 47,000 OIA requests Police received in that period to confirm the number of Privacy Act requests that were incorrectly logged, that number is refused under section 18(f) of the OIA as the information requested cannot be made available without substantial collation or research.

The average response time for those requests that have been responded to as of 3 November 2022 was 12.4 days.

Of the requests which have been responded to as of 3 November 2022, 2639 were refused in full.

As IRT does not record the reasons for refusal in a searchable field, it would require manually reviewing 2639 individual files to identify reasons for refusal in each case. That information is therefore refused under section 18(f) of the OIA, as the information requested cannot be made available without substantial collation or research.

Please note this data is sourced from a dynamic operational Police system and is subject to change.



In the period 1 February 2021 to 31 July 2022, the Office of the Privacy Commissioner closed 43 complaints that related to a Police decision on a Privacy Act request. Of these, 21 resulted in the release of further information by Police.

2. *Any internal guidance, policies, procedures, decision papers or other material which is or might be used by Police in determining if they are correctly responding to requests and complying with the Privacy Act. For clarity, this includes any material which helps an officer decide to decline or approve a request, what information to release, and what grounds can be relied upon for refusing to release.*

Please find attached Police Instruction – *Disclosure under the Privacy Act 2020*.

3. *Any internal escalation or review of this process or decisions made by individuals responding to privacy act requests on police's behalf.*

The *Disclosure under the Privacy Act 2020* Police Instruction was last updated on 1 December 2020.

Once Police issues its decision on a Privacy Act request it would not typically review that decision except where it receives a complaint from the Office of the Privacy Commissioner.

4. *Any documentation relating to steps Police take to ensure information they receive is only "linked" to the correct person that information is about. For clarity this includes how police determine the natural person involved and how police ensure the identity information is correct and accurate to an individual.*

Please refer to Police Instruction – *Collection of Personal information*, which is publicly available here: <https://www.police.govt.nz/about-us/publication/collection-personal-information-police-manual-chapter>

5. *Any documentation relating to how an individual's identity is confirmed in NIA or other Police applications.*

Your request for documentation about how Police confirms identity in the National Intelligence Application (NIA) is refused pursuant to section 18(e) as a document containing the information requested does not exist.

Police use a variety of procedures to confirm an individual's identity in NIA. Our call takers or an officer would seek verification against additional information (e.g., a date of birth, driver's licence number, address, or last contact with Police). In the cases of individuals under arrest there are provisions to take identifying details such as fingerprints or DNA which would then allow for a match against the information held in NIA.

Additionally, there are provisions to access identity information from other agencies. For example, Driver's Licence photos from Waka Kotahi.

The *Identity Information Sharing* Police Instruction is attached.

6. *Any documentation relating to steps taken by Police to ensure section 6 privacy act requests are only released to the correct person, with particular interest in areas where identity is questionable such as people with the same name and date of birth.*

The requirements to establish identity are set out on our website at <https://www.police.govt.nz/advice-services/request-information/request-information-about-yourself-privacy-act> under the Evidence of identity section.

Please refer also to the attached *Disclosure under the Privacy Act 2020* Police Instruction.

You have the right to ask the Ombudsman to review my decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Zane Kearns', with a long horizontal flourish extending to the right.

Zane Kearns
Director - Service
New Zealand Police

Identity information sharing

Table of Contents

Table of Contents	2
Policy statement and principles	4
What	4
Why	4
How	4
Overview	5
Introduction	5
Purpose of identity information sharing chapter	5
Legislation permitting identity information sharing	5
Purpose of information sharing	5
Relationship between 'identity information' and other law relating to information disclosure	5
Accessing agencies	5
Purpose of access	5
Manner and form of access	6
Related information	6
Definitions and acronyms	8
Table of definitions and acronyms	8
Access	8
Accessing agency	8
Act	8
BDMRR Act	8
Biometric information	8
Database	8
DIA	8
DL images	8
Holder agency	8
Identifying information	8
Identity information	9
INZ	9
MBIE	9
NIA	9
NZTA	9
'OnDuty'	9
Personal information	9
Police information	9
INZ: Police process for identity information sharing	10
Introduction	10
Querying an identity with INZ	10
Linking Police and INZ identities in NIA	10
Police query criteria	10
Procedure for accessing identity information from INZ	11
Process for disclosing Police information to INZ	11
Related information	12
NZTA: Police process for accessing driver licence photographs	13
Introduction	13
Police access criteria	13
Procedure for accessing driver licence photographs from NZTA	13
Dual or multiple identities	13
Police use and disclosure of NZTA identity information	14
Storage of DL images	14
Retention of DL images	14
DIA and Registrar-General, Births, Deaths and Marriages: Police process for accessing identity information	15
Introduction	15
Police access criteria	15
Sharing under Part 7 (subpart 2) of the Privacy Act	15
Sharing under section 78AB of the BDMRR Act	15
Information shared and not shared	16
Procedure for accessing identity information from DIA	16

Police use and disclosure of DIA identity information	17
Linking a DIA passport identity to a NIA person	18
Unlinking a DIA passport identity to a NIA person	18
Retention and storage of DIA identity information	18
Obtaining information not accessible electronically	18
Authority to access	18
Certificates	18
Access requirements and restrictions	18
Monitoring	19
Registrar-General, Births, Deaths and Marriages: Non-disclosure direction	20
Non-disclosure direction background	20
Requests for non-disclosure direction	20
Advice given to applicants for non-disclosure direction	20
When application is approved	20
Effect and duration of non-disclosure direction	20
Purpose of Registrar-General sharing non-disclosure direction information with Police	20
Police receiving non-disclosure direction information from the Registrar-General	21
Content of non-disclosure direction information	21
Protecting non-disclosure direction information	21
Related information	22

Policy statement and principles

What

Part 7 (subpart 2) of the [Privacy Act 2020](#) regulates identity information sharing including photographs of persons (e.g. driver's licence photograph).

This chapter provides policy and procedures for Police employees relating to identity information sharing with:

- Immigration New Zealand
- New Zealand Transport Agency
- Department of Internal Affairs.

Why

The effective and timely exchange of [identity information](#) enables Police to manage identity that contributes towards combatting organised crime, transnational and other crime impacting on New Zealand.

How

Police:

- will ensure the information sharing requirements of the Privacy Act are complied with
- will follow the query criteria outlined in this chapter or under an MOU before instigating a person of interest query
- will access [identity information](#) under section 165 electronically (using NIA or 'On Duty') from the [holder agency](#) in the manner agreed with the agency (note: access is direct to information stored in a holder agency's database)
- will retain, manage and secure [identity information](#) in accordance with the Privacy Act and the [New Zealand Information Security Manual](#)
- will note and comply with restricted access when using online queries in 'NIA' and 'Mobility'
- may disclose Police information subject to certain legal and policy criteria being met
- may use [identity information](#):
 - to identify a person of interest
 - to check matters relating to a person of interest
 - as authorised by law, e.g. as part of a criminal investigation for the purposes of maintaining the law.

Overview

Introduction

This chapter provides the process for accessing and sharing [identity information](#) from:

- New Zealand Transport Agency (NZTA) relating to driver licence photographs
- Immigration New Zealand (INZ) relating to an individual's identity and New Zealand travel documents
- Department of Internal Affairs (DIA)
- Secretary of Internal Affairs relating to passports
- Registrar-General of Births, Deaths, and Marriages relating to:
 - births, deaths and marriages
 - name change
 - death notification.

Note: Identity information includes photographs of persons (e.g. driver's licence/passport photograph).

Purpose of identity information sharing chapter

The purpose of this chapter is to guide and support effective and timely exchange of information that is appropriate and necessary to:

- combat organised, transnational and other crime that impacts upon New Zealand
- protect New Zealand's interests such as immigration compliance activities enforced by INZ
- manage identity information as it relates to persons entering/in the justice system.

Legislation permitting identity information sharing

Purpose of information sharing

The purpose of the 'identity information sharing part' of the Privacy Act 2020 is to authorise [accessing agencies](#), when carrying out specified functions, to verify the identity of an individual by accessing [identity information](#) held about that individual by a [holder agency](#).

(s [162](#))

Relationship between 'identity information' and other law relating to information disclosure

Part [7](#) (subpart 2) (identity information) of the Act does not:

- limit the collection, use, or disclosure of personal information that:
 - is authorised or required by or under any enactment; or
 - is permitted by the information privacy principles:
- limit the following 'Parts' of the Act:
 - part [7](#) (subpart 1) (information sharing)
 - subpart [4](#) (information matching)
 -
 - subpart [3](#) (law enforcement information).

(s [163](#))

Accessing agencies

Accessing agencies are permitted to access [identity information](#) under section [165](#) of the Privacy Act 2020:

"An accessing agency may, for the purpose specified in the second column of Schedule [3](#) opposite the name of the accessing agency, have access to an individual's identity information held by a holder agency specified in the third column of that schedule opposite the name of the accessing agency."

Purpose of access

This table outlines the [accessing agency](#) and the purpose for which access is sought from the [holder agency](#).

Accessing agency	Purpose of access	Holder agency
INZ	<p>To verify the identity of a person</p> <ul style="list-style-type: none"> - who is seeking to travel to New Zealand - who is arriving in or departing from New Zealand - who is applying for a visa - who an immigration officer has good cause to suspect: <ul style="list-style-type: none"> - has committed an offence against the Immigration Act 2009 - has obtained a visa under a fraudulent identity - is liable for deportation or turnaround - is unlawfully in New Zealand. 	Police
Police	<p>To verify the identity of a person:</p> <ul style="list-style-type: none"> - whose identifying particulars have been taken under section 32 (identifying particulars of person in custody) or 33 (identifying particulars for summons) of the Policing Act 2008 - whose identifying particulars have been taken under section 11 of the Returning Offenders (Management and Information) Act 2015 - who has breached, has attempted to breach, or is preparing to breach a condition of any sentence, or order imposed under any enactment, that the person not leave New Zealand. <p>Note: Where the circumstances above are not met, NZP may request identity information from INZ and INZ may disclose identity information:</p> <ul style="list-style-type: none"> - to avoid prejudice to the maintenance of the law (Information Privacy Principle 11(e)(i)); or - for the conduct of court or tribunal proceedings (Information Privacy Principle 11(e)(iv)); or - to prevent or lessen a serious threat to public health or public safety or the life or health of an individual (Information Privacy Principle 11(f)). 	<ul style="list-style-type: none"> - INZ - NZTA - DIA

Note: NZTA is not an accessing agency under schedule [3](#) of the Privacy Act.

Manner and form of access

Access under section [165](#) may be facilitated between a [holder agency](#) and an [accessing agency](#) in the **manner agreed** by the agencies (for example, by direct access to information stored in a holder agency’s database, or by exchange of information between the agencies).

Note: Manner agreed by the agencies is by electronic means with Police using ‘On Duty’ or NIA.

Identity information that is held by a holder agency and accessed by an accessing agency under section [165](#) may be made available to the accessing agency in the form agreed by the agencies.

(s [166](#))

Related information

See also these Police Instructions:

- [Information Sharing Agreement between Registrar-General \(BD&M\) and New Zealand Police](#)
- [MBIE MOU, Schedule INZ4: Information sharing](#)
- [Police-DIA MOU, Schedule 1: Information sharing](#)
- [Police-NZTA MOU, Schedule 11: Police access to driver licence images](#)
- [Privacy and official information](#) chapters
- [Information security and assurance](#)
- [Police information and records management policy](#)

- Criminal disclosure
- Departmental security.

Definitions and acronyms

Table of definitions and acronyms

This table defines key terms and acronyms.

Term	Description
Access	Access, in relation to a database, includes remote access to that database. (s 164)
Accessing agency	Accessing agency means an agency specified in the first column of Schedule 3 . (s 164) Note: Accessing agency includes Police and INZ, but not NZTA or DIA.
Act	Act means the Privacy Act 2020 .
BDMRR Act	Births, Deaths, Marriages, and Relationships Registration Act 1995
Biometric information	Biometric information, in relation to a person, means information that comprises: <ul style="list-style-type: none"> - 1 or more of the following kinds of personal information: <ul style="list-style-type: none"> - a photograph of all or any part of the person's face and shoulders - impressions of the person's fingerprints, palmprints - a scan of the person's irises; and - an electronic record of the personal information that is capable of being used for biometric matching (s 164)
Database	Database means any information recording system or facility used by an agency to store information. (s 164)
DIA	Department of Internal Affairs
DL images	Driver licence photographs held by NZTA.
Holder agency	Holder agency means an agency specified in the third column of Schedule 3 . (s 164)
Identifying information (accessing agency)	Identifying information is the following details that an accessing agency (is usually Police, but may involve a request from INZ) must provide to the holder agency: <ul style="list-style-type: none"> - full name - date of birth - gender.

<p>Identity information (holder agency)</p>	<p>Identity information, in relation to an individual, means any information that identifies, or relates to the identity of, the individual, and includes (without limitation) the following information:</p> <ul style="list-style-type: none"> - the individual’s biographical details (for example, the individual’s name, address, date of birth, place of birth, and gender) - the individual’s biometric information - a photograph or visual image of the individual - details of the individual’s: <ul style="list-style-type: none"> - New Zealand travel document; or - certificate of identity - details of any distinguishing features (including tattoos and birthmarks). <p>(s 164)</p>
<p>INZ</p>	<p>Immigration New Zealand</p>
<p>MBIE</p>	<p>Ministry of Business Innovation and Employment</p>
<p>NIA</p>	<p>National Intelligence Application: a critical system that supports a wide range of Police operational processes.</p>
<p>NZTA</p>	<p>New Zealand Transport Agency</p>
<p>‘OnDuty’</p>	<p>‘On Duty’ is an application that is used through Police mobility devices (e.g. iPhones) for making queries and submitting intel notings.</p>
<p>Personal information</p>	<p>Personal information means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act (as defined by the BDMRR Act).</p> <p>(s 7)</p>
<p>Police information</p>	<p>Police information is information held by Police and includes:</p> <ul style="list-style-type: none"> - Police officer identifier; - Police officer assigned station; - custody station name; - unique identifying number used by NZP; - Australia & New Zealand offence code (ANZOC) Level 2 Offence Code (if person is being charged); - prisoner type; - court date (if applicable); - court location (if applicable) - person of interest identity information that Police provide to INZ.

INZ: Police process for identity information sharing

Introduction

The agreed process for sharing [identity information](#) and [police information](#) between Police and Immigration New Zealand (INZ) involves:

- Police providing [identifying information](#) of persons of interest and INZ, if satisfied with the Police request, disclosing identity information about that person; and
- Police disclosing police information about a non-New Zealander to INZ for compliance purposes.

Querying an identity with INZ

When querying an identity with INZ through NIA, INZ will compare the [identifying information](#) supplied by Police with their own information. If there is a possible match INZ will reply with disclosed [identity information](#) that may or may not correspond to the person of interest to Police. Be aware that the returned identity information could involve an unrelated person.

Linking Police and INZ identities in NIA

Before linking NIA and INZ identities you must be **absolutely certain** that the NIA and INZ identities relate to the same person. The NIA biographics (name, DOB, nationality) and biometrics (photo where available - Police/NZTA) should be the same as those of the INZ identity.

Police query criteria

The criteria for querying [identity information](#) about a person of interest with INZ varies whether done electronically or manually. An electronic query is the preferred option (Option 1 below). If those criteria are not met, then consider the wider criteria of the second option (manual query) and use that when criteria are met.

<p>Option 1</p>	<p>Electronic query criteria (Using 'OnDuty' or 'NIA')</p>	<p>Verification is sought of a person of interest's identity;and</p> <p>Either:</p> <ul style="list-style-type: none"> - the person: <ul style="list-style-type: none"> - has had their identifying particulars taken under section 32 or 33 of the Policing Act 2008 (custody or summons); or - has had their identifying particulars taken under section 11 of the Returning Offenders (Management and Information Act 2015 (as a returning offender); or - has breached (or attempted) a sentence or order not to leave New Zealand. <p>Or</p> <ul style="list-style-type: none"> - Police requires the information: <ul style="list-style-type: none"> - for the purpose of maintaining the law;or - to prevent or lessen a serious threat to the health or safety of a person or the public;or - for the conduct of court or tribunal proceedings.
<p>Option 2</p>	<p>Manual query criteria (extended criteria)</p>	<p>Verification is sought of a person of interest's identity;and</p> <ul style="list-style-type: none"> - the person: <ul style="list-style-type: none"> - is liable to an infringement notice; or - may be a victim or witness; or - is of interest to Police <p>and</p> <ul style="list-style-type: none"> - INZ receiving the query is satisfied that Police has a need for the information: <ul style="list-style-type: none"> - for the purpose of maintaining the law;or - to prevent or lessen a serious threat to the health and safety of a person or the public;or - for the conduct of court or tribunal proceedings.

Procedure for accessing identity information from INZ

Follow these steps for accessing [identity information](#) from DIA.

Step	Action
1	<p>Query INZ by ensuring to use:</p> <ul style="list-style-type: none"> - first option where electronic criteria are met: - electronically ('OnDuty' or 'NIA', e.g. Query Person > Identity Information > External Agency Links > then click on 'Query INZ' button) - second option: if electronic criteria not met, by contacting an INZ employee directly (e.g. phoning INZ's 0800 274 274 number - help desk) with identifying information to establish or verify the person of interest's identity, including travel movements.
2	<p>Ensure one of the Police query criteria is met before instigating a person of interest query with INZ.</p>
3	<p>Establish/collect the person's full name, date of birth and gender.</p>
4	<p>Be aware that the returned identity information from INZ:</p> <ul style="list-style-type: none"> - may or may not correspond to the person of interest being queried - could involve an unrelated person.

Process for disclosing Police information to INZ

Police may disclose [Police information](#) about a non-New Zealander either electronically when linking an INZ identity to a Police identity, or by directly contacting INZ (Compliance Officer) by landline, mobility device or email, where:

- it reasonably believes there is a high likelihood it holds Police Information about the relevant person; and
- there is a reasonable basis for the disclosure; and
- there is a reasonable belief that the information being disclosed is accurate; and
- there are no operational and/or legal reasons not to disclose the information (for example if the information is about a young person and there are proceedings before the Youth Court).

Note: Police information about children and young persons in NIA will not be automatically generated in the system or disclosed to INZ. However, there may be special circumstances when the information may be disclosed to INZ directly.

Related information

See also the annex located in [Schedule INZ4: Information sharing](#) with Immigration New Zealand (INZ) of the [Memorandum of Understanding between Ministry of Business Innovation and Employment \(MBIE\) and Police](#) for further information.

NZTA: Police process for accessing driver licence photographs

Introduction

This section sets out the agreed process, practice and procedures for Police to lawfully access drivers licence photographic images (DL images) from the New Zealand Transport Agency (NZTA) database.

See also [Police-NZTA MOU](#), [Schedule 11: Police access to driver licence images](#) for the formal agreement with Police accessing DL images.

Police access criteria

Police employees must only access DL images of a person of interest from NZTA in the course of their official duties to verify the identity of a particular individual for the purpose of law enforcement, in accordance with section [200\(4\)](#) of the Land Transport Act.

Procedure for accessing driver licence photographs from NZTA

Police access to DL images is available to all Police employees electronically through NIA and the 'On Duty' application available on Police mobility devices (e.g. iPhone and iPad).

Follow these steps for a quick response without burdening NZTA employees:

Step	Action
1	Query through either the Query Person Application on Police Mobility Devices or through desktop access to NIA: - Query Person > Identity Information > NZTA Driver's Licence
2	Use the following information fields: - driver licence number - QID - date / time.
3	Note the returning response of the latest DL image(s) will match the driver licence number(s) you provided. The following fields will be returned with the DL image(s): - driver licence number - image ID - when captured date - image.
4	Be aware that suspected dual or multiple identities are notified to Police by NZTA through email (DriverLicencePhoto@police.govt.nz). If a notification is received, you will be sent a query asking if the dual or multiple identities are relevant to your enquiry. See ' Dual or multiple identities ' for further information about the notification, query sent to you and how your reply will influence NZTA response to avoid jeopardising the Police enquiry.

Dual or multiple identities

If the NZTA suspect dual or multiple identities based on the DL image as a result of a request from Police, then the NZTA will advise Police by email (DriverLicencePhoto@police.govt.nz) of the possible dual or multiple identities when responding to the request.

In receipt of the notification from NZTA of possible dual or multiple identities, the Police recipient monitoring the email site must advise the requesting Police employee to determine whether the dual or multiple identities are relevant to the Police enquiry. Where it is determined:

- **relevant**, the requesting Police employee must advise NZTA by email (DLimages@nzta.govt.nz)

Note: The NZTA agree to suspend their standard processes for dual or multiple identities. Once completed, the requesting Police employee notifies NZTA by email and the NZTA will commence their standard processes for dual or multiple identities.

- **not relevant**, the requesting Police employee must advise the NZTA by email and the NZTA will commence their standard processes for dual or multiple identities.

Police use and disclosure of NZTA identity information

DL images accessed from NZTA may be used by Police:

- to verify the identity of a person of interest
- to check matters relating to a person of interest
- as authorised by law, e.g. as part of a criminal investigation for the purposes of maintaining the law; or
- to disclose to a corresponding overseas agency under either an international disclosure instrument made under section 95B of the Policing Act 2008 or directions issued by the Commissioner under section 95C of the Policing Act 2008.

Where NZTA drivers' licence photographs are incorporated into reports or documents (e.g. photo line-ups, intel documents) for further distribution either within Police or to other agencies, this information is to be dealt with in accordance with any relevant caveats, including relevant restrictions or conditions, and legislation relating to its lawful distribution (e.g. Information Privacy Principle [11](#)(e)(i) of the Privacy Act 2020 to avoid prejudice to the maintenance of the law).

Note: Requests from other agencies for NZTA DL images from Police must be declined. The requestor should be advised to make their request direct to NZTA, unless the request forms part of a joint operation with Police (e.g. joint Police/Customs drug delivery operation).

Storage of DL images

Police employees must not store DL images provided by NZTA in a separate collection/database for later use.

Retention of DL images

Police employees must ensure DL images received from NZTA are managed in accordance with:

- the Privacy Act 2020
- Police security and privacy policies, practices, and procedures
- the New Zealand Government security protocols such as the [New Zealand Information Security Manual](#).

DIA and Registrar-General, Births, Deaths and Marriages: Police process for accessing identity information

Introduction

This section sets out the agreed process, practice and procedures for Police to lawfully access [identity information](#) and associated images relating to births and passports from the Department of Internal Affairs (DIA):

- Secretary of Internal Affairs (for passports)
- Registrar-General of Births, Deaths and Marriages.

Note: Identity Information relating to deaths and name changes are not accessible online at this time, but it is planned they will become available later. In these cases see the manual process in [Obtaining information not accessible electronically](#) below.

See also [Police-DIA MOU, Schedule 1: Information sharing](#) for the formal agreement with Police accessing identity information and associated images.

DIA and the Registrar-General are permitted to share [identity information](#) under:

- section [78AB](#) of the Births, Deaths, Marriages, and Relationships Registration (BDMRR) Act 1995
- Part [7](#) (subpart 2) of the Privacy Act 2020

Police access criteria

Police employees must only access [identity information](#) for policing and law enforcement purposes as authorised by or under law when a person:

- is liable to detention, arrest, or summons, or
- has breached (or attempted) any sentence, conviction or order, or
- is a suspect or offender for an offence and verification is sought of their identity (note, this reason cannot be used for querying of birth records).

Sharing under Part 7 (subpart 2) of the Privacy Act

Police are authorised to receive information from the Registrar-General and/or DIA to verify the identity of a person:

- whose identifying particulars have been taken under section [32](#) (identifying particulars of person in custody) or [33](#) (identifying particulars for summons) of the Policing Act 2008;
- whose identifying particulars have been taken under section [11](#) of the Returning Offenders (Management and Information) Act 2015;
- who has breached, or has attempted to breach, or is preparing to breach a condition of any sentence, or order imposed under any enactment, that the person not leave New Zealand.

The types of information include biometric and identity information, as defined by section [164](#) of the Privacy Act 2020.

Sharing under section 78AB of the BDMRR Act

Police may request personal information held by the Registrar-General on an individual where Police suspects that the individual:

- is, or is liable to be, detained under an enactment
- is, or is liable to be, arrested under a warrant issued by a court or any court Registrar
- is contravening, or is about to contravene, an enactment or a court order
- is liable to be prosecuted for an offence punishable by imprisonment
- is, or is liable to be, detained or arrested in respect of a traffic offence
- is endangering, or is threatening to endanger, the life, health, or safety of a person or group of persons
- is injured or is dead.

The personal information Police may request from the Registrar-General is a subset of the following information held by the Registrar-General:

- registered birth information
- registered death information
- registered marriage information
- registered civil union information
- registered name change information.

Information shared and not shared

See the **MOU with DIA** [Appendix A - Information to be shared between the Registrar-General and Police](#) or [Appendix B - Information to be shared between the Secretary of Internal Affairs and Police](#) for information about what can be shared and matching rules.

Procedure for accessing identity information from DIA

Follow these steps for accessing [identity information](#) from DIA.

Step	Action
1	<p>Query DIA by using:</p> <p>Preferred first option when criteria met: electronically ('OnDuty' or 'NIA', e.g. Query Person > Identity Information > External Agency Links > then click on 'Query DIA' button). The following query criteria have to be met before instigating a person of interest query with DIA through NIA or OnDuty:</p> <ul style="list-style-type: none"> - person is liable for detention, arrest or summons - person is in breach (or attempted) of any sentence condition or order - to verify suspect or offender identity (note, this reason cannot be used for querying of Birth records). <p>second option - if criteria are not met: contacting a DIA employee directly (e.g. phoning 'Births, Deaths & Marriages' 0800 22 52 52 number or 'Passports' 0800 22 50 50) with identifying information to establish or verify the person of interest's identity. Note: Querying birth records can only be done through this option</p>
2	<p>Establish/collect this identifying information:</p> <ul style="list-style-type: none"> - first name(s) (optional) - surname - date of birth - gender <p>Also provide to the DIA:</p> <ul style="list-style-type: none"> - requesting Police Officer ID - requesting Officer's HR location - query reason: <ul style="list-style-type: none"> - this will be providing one of the following fields to the Registrar-General (Births, Deaths & Marriages): <ul style="list-style-type: none"> - 'query person' - when querying an individual outside of the custody module - 'query custody' - when querying an individual within the custody module (Note: For birth identity data, the Birth Registration Number field in the birth record results cannot be provided to Police, so is displayed as "Birth Registration #: 9999999999") - this will be providing one of the following fields to the Secretary of Internal Affairs (Passports): <ul style="list-style-type: none"> - 'query Person' - querying an individual outside of the custody module - 'view details' - selecting a specific item from a result list outside of the custody module - 'retrieve' - requesting 'the latest' details for a linked identity or when selecting a specific identity from a result set outside of the custody module - 'query custody' - when querying an individual within the custody module (Note: For birth identity data, the Birth Registration Number field in the birth record results cannot be provided to Police, so is displayed as "Birth Registration #: 9999999999") - 'view details custody' - selecting a specific item from a result list inside of the custody module. - 'retrieve custody' - requesting 'the latest' details for a linked identity within the custody module. <p>Note: A DIA Passport query can be by Passport number or Name. If queried by Passport Number the result will relate to that passport which may not be the current passport held. Querying by 'name' will return the most recent passport if a match is found.</p> <p>Note: For queries by 'name', because of limitations imposed by the DIA system, DIA will only return results that are exact matches to the name entered (unlike NIA and OnDuty). If a match is not found, alternative spelling or combinations of the name should be tried. Alternatively, INZ may be queried with identifying information and if the NZ citizen has travelled outside the country, their identity and NZ passport number will be supplied to enable a passport number query with DIA to obtain the passport details and photograph.</p>

Police use and disclosure of DIA identity information

Identity information accessed from DIA or the Registrar-General may be used by Police:

- to verify the identity of a person of interest
- to check matters relating to a person of interest
- as authorised by law, e.g. as part of a criminal investigation for the purposes of maintaining the law; or
- to disclose to a corresponding overseas agency under either an international disclosure instrument made under section 95B of the Policing Act 2008 or directions issued by the Commissioner under section 95C of the Policing Act 2008.

Police may disclose access information pursuant to any other information sharing agreement or enactment, including the ability to access identity information pursuant to the Privacy Act 2020.

Information that is provided to any third party as authorised by or under law will be provided on the basis of any relevant restrictions or conditions.

Where any information is incorporated into reports or documents for further dissemination then that information will be dealt with in accordance with any relevant caveats and legislation relating to its lawful distribution.

Linking a DIA passport identity to a NIA person

If a DIA identity found through a query is believed to be the same person as the NIA person the query has been run for e.g. the passport photo (where available), names etc. correspond, as does country, date, and place of birth, then the user has an option to link the DIA passport identity to the NIA person. This linking should only be done where you are satisfied that there is no doubt that the DIA passport identity and the NIA person are the same person.

DIA birth records cannot be linked to a NIA person.

To link a DIA identity to a NIA person, use the 'external agency' node on the person dossier/record view. Linking can also be done via a Custody record.

Unlinking a DIA passport identity to a NIA person

If viewing the DIA passport details for a linked identity to a NIA person, a user can unlink that identity if they decide the NIA person and DIA passport do not correspond or there is a more relevant/recent passport identity for that person.

Retention and storage of DIA identity information

Police employees receiving identity information from DIA or the Registrar-General may use the information to correct and update records held by Police.

Information will be retained by Police in accordance with public record keeping requirements of the Public Records Act 2005.

Information received from DIA will be stored by Police in a secure Police enterprise system that protects the information against unauthorised use, modification, destruction, access and disclosure or any other misuse.

Information shared by DIA will be disposed of as soon as it is no longer required for the purposes specified in this Schedule, or as otherwise required by law.

Obtaining information not accessible electronically

National Criminal Investigations Group (NCIG) provide a service whereby searches can be made of the Register of Births, Deaths, Marriages, Relationships and name changes which is a Department of Internal Affairs database. National Biometrics Information Office staff travel to the Internal Affairs offices to carry out these searches. Note: The database is not accessed by way of the Police computer system.

Authority to access

Searches are subject to the Births, Deaths, Marriages and Relationships Registration Act 1995, specifically section 74. Searches are carried out by and for Police on the authority of the Registrar General and certificates are produced at no cost to Police.

Certificates

Certificates are not produced immediately, but are forwarded by Internal Affairs to National Biometrics Information office some days after being requested. This means you need to plan well ahead especially if they are required for court purposes or similar. An adjournment may be necessary.

Access requirements and restrictions

Police can only access the database during business hours (Monday to Friday, 9am to 5pm) and then only when a computer terminal is available.

These requirements must be met to enable searches. The search request:

- must be made on the approved form under 'Notification' in Ten-One entitled "Query Birth, Death, Marriage, Civil Union Register". This provides an audit trail.
- Note: Incomplete requests or requests by email or phone will not be actioned.
- must be for Police purposes, that is, assisting with the investigation and detection of criminal offences. The reason must be stated on the request (a narrative box is provided). The exact operational reason must be provided.
- Note: Requests should only be made when other investigative options have been exhausted.
- must not be carried out on behalf of another agency. Coroners for example have their own business relationship with Department of Internal Affairs
- must be on a named person, and only on a named person (this is a legislative requirement)
- must not be on a person in order to find their child's birth record. The correct procedure is to search the child
- may be on a person in order to determine their parents; it is not acceptable to then search those parents to find other children or siblings.

Important: *"To find out who the grandparents/father/mother/aunt/uncle/siblings and children of the person" is generally not a valid reason. Exceptions to this general requirement may apply in very special cases. The Registrar may carry out a search for example in the case of familial DNA and higher level criminal profiling. These requests, due to the serious nature of the offending will be rare and will only be actioned when routed through the Manager: National Forensic Services at NCIG, PNHQ.*

Monitoring

Compliance with these instructions is monitored by the Director: NCIG.

Registrar-General, Births, Deaths and Marriages: Non-disclosure direction

There is an '[Information Sharing Agreement between Registrar-General Births Deaths and Marriages and New Zealand Police](#)' to enable the Registrar-General to disclose to the Police, personal information relating to [non-disclosure direction information](#).

Non-disclosure direction background

Requests for non-disclosure direction

A person or their [personal representative](#) who is the subject of birth information, marriage information, civil union information or name change information may request a non-disclosure direction from the Registrar General (section [75A](#) of the Births, Deaths, Marriages, Relationships Registration Act 1995).

Advice given to applicants for non-disclosure direction

If people think that public access to their records would put them or their family in danger, they can apply for a non-disclosure direction.

Applicants are advised that:

- A non-disclosure direction means that the only people who can access their records are:
 - themselves
 - authorised government departments doing their regular work
 - their parent or guardian if they are under 18
 - their power of attorney if they have one.
- Anyone else who tries to request their records will be advised that the information exists but cannot be given to them.
- A non-disclosure direction lasts for 5 years.
- Details about current non-disclosure directions may be shared with authorised government departments so they can add extra safeguards to their information.
- If they have a non-disclosure direction and they make any part of their information publicly available, anyone can then ask Births, Deaths and Marriages to verify whether that information matches their registered information.

When application is approved

When applicants' non-disclosure applications are approved, the Registrar-General Births, Deaths and Marriages sends a letter reminding them that the Department of Internal Affairs (DIA) does not contact them to reinstate their non-disclosure direction. To reinstate or withdraw the non-disclosure direction, applicants must complete a further application.

Effect and duration of non-disclosure direction

Any person requesting information who is **not** the subject of that information, nor that person's personal representative, will be advised by the Registrar General that the information exists, but cannot be complied with because a non-disclosure direction is in force. (s[75B](#)(2))

Under section [s75B](#)(3) a non-disclosure direction is in force from the date on which the Registrar-General gives the direction until the earlier of:

- the expiry of the prescribed period, or
- a date the Registrar-General directs that the direction be withdrawn.

The duration is 5 years unless renewed. The Registrar General does not remind the person to make a subsequent application to reinstate their non-disclosure direction when the duration period is about to terminate.

Purpose of Registrar-General sharing non-disclosure direction information with Police

The purpose of the Registrar-General sharing non-disclosure direction information with Police is to assist Police in performing its functions relating to the maintenance of the law including enabling Police to:

- correctly identify individuals (e.g, by linking identities, or detecting and correcting false identity information); and
- protecting the identity of individuals who have a non-disclosure direction in force in respect of their birth or name change

information.

Police receiving non-disclosure direction information from the Registrar-General

The Registrar-General provides Police National Headquarters (PNHQ) (National Biometric Information Office) with approved non-disclosure direction information, and separate notification when that information expires in a secure manner. PNHQ, on receipt of that information will:

- run a match of the information against current information in NIA
- in the event of a successful match, amend the person's record in NIA to reflect the received information (this will include an indicator that the individual has a non-disclosure direction in force)
- in the event of an unsuccessful match for a new non-disclosure direction, create a new record in NIA and include the indicator for a non-disclosure direction
- indicate in NIA that the information was provided by the Registrar-General (Births, Deaths and Marriages)
- when notified of non-disclosure direction (NDD) expiry, remove that NDD indicator from NIA.

Content of non-disclosure direction information

Updated records of non-disclosure direction information in NIA is accessible to Police employees for maintenance of the law. Information content includes:

- first name(s) at birth
- surname at birth
- former first name(s)
- former surname(s)
- new first name(s)
- new surname
- date of birth
- place of birth/country of birth
- sex
- home address of parent 1 at birth
- home address of parent 2 at birth
- address at time of name change
- date non-disclosure direction comes into force
- non-disclosure direction end date
- record type (R - Registration or C - Correction).

Protecting non-disclosure direction information

Non-disclosure direction information relating to a person's identity recorded in NIA is accompanied with a notation to that effect (i.e. the individual has a non-disclosure direction in force). That information **may only be used** for any of the following purposes:

- maintenance of the law including prevention, detection, investigation, and prosecution of offences (also encompasses detention and/or arrest of a person),
- preventing or lessening a serious or imminent threat to:
 - public health or public safety, or
 - the life or health of the individual concerned or another individual, or
 - any court or tribunal proceedings that have been commenced or are reasonably in contemplation.

([s22](#), principle 10 of the Privacy Act 2020)

See also '[section 7. Adverse actions](#)' of the 'Approved Information Sharing Agreement between Registrar-General and New Zealand Police'.

Police employees must not disclose non-disclosure direction information to other parties, unless when necessary for law enforcement purposes and in accordance with legislation. If in doubt then seek guidance from your supervisor/manager or local

Legal Advisor before disclosing that information to other parties.

In the event of a privacy breach, follow the guidance in the ['Privacy breach management'](#) chapter.

Related information

See also these Police Instructions:

- [Criminal disclosure](#)
 - [Information Sharing Agreement between Registrar-General and New Zealand Police](#)
 - [Police-DIA MOU, Schedule 1: Information sharing](#)
 - [Privacy and official information](#) chapters.
-

Disclosure under the Privacy Act 2020

Table of Contents

Table of Contents	2
Introduction	6
Purpose of this chapter	6
Personal information defined	6
When does the Privacy Act apply?	6
References to 'the Act'	6
Purpose of the Privacy Act	6
Information privacy principles relevant to disclosure	6
Related information	7
Information Request Tool (IRT) Guides	7
Other resources	7
Requests for personal information	8
Who can make a request	8
Identifying the requester	8
Verifying identity in person	8
Primary and secondary IDs	8
Verifying identity via a trusted referee	8
Requests for correction of personal information	9
IPP6 and IPP7 do not apply to certain information	9
Form of the request	9
Time limits for responding to requests	9
Extension of time limit	9
Key roles and responsibilities	10
Oversight at PNHQ	10
End-to-end oversight in Districts	10
Preparing the response	10
At PNHQ	10
In Districts	10
How to action a Privacy Act request - an overview of the processing stages	11
Key process points	11
What you need to know	11
Key Timeframes	11
Remember	11
Logging a Privacy Act request	12
Triaging and assigning requests	13
Matters to consider during triage	13
Transfer - does the request belong with Police or another agency? [by day 10]	13
Requests for criminal conviction histories	13
Is the correct District handling the request?	15
Confirm the requester's identity	15
Is the request confidential?	15
Is there a high organisational impact?	15
Timeframes and extensions	15
Urgent requests	15
Are there likely to be problems reaching a decision on the response within 20 working days?	15
Extensions - when you can extend the time to respond to a request?	15
How to notify an extension	15
Acknowledge the request	16
Assigning Privacy Act requests and accepting responsibility	16
Privacy Act template letters	16
Checklist for logging and triaging a request [by day 3]	16
Scoping the information	18
Clarify the request [by day 7]	18
Check for previously released information to the requester	18

Plan your timeline	18
Identify who you need input from and who to consult	18
Identify whether the information exists, its location, how much there is likely to be, and how long it will take to get/assess it	18
Identify any risks or impacts with the type of information requested	18
Relevant templates	18
Collating the information	20
Identify information in scope	20
Collect copies of the information in scope	20
Issues that may come up during collation	20
Information is not readily retrievable or not held	20
Information does not exist or cannot be found	20
Large volumes of information	21
Information requested in the course of criminal proceedings	21
Limits on charging for providing personal information	21
Statutory protection when releasing information in good faith	21
Relevant templates	21
Checklist for collating the information	[by week 1-2] 22
Compiling the response	23
Consider if any information should be withheld or the request refused	23
Consider how personal information can be made available?	23
How has the requester asked for the information?	23
Consulting with others	23
Making a decision	24
Compiling the information for release	24
Drafting a response letter	24
Reviews	25
Supervisor review	25
Legal review	25
Following completion of any reviews	25
Relevant templates	25
Finalising/approvals (PNHQ/Districts)	27
Approval before release	27
Use a secure method of disclosure	27
Releasing the response	27
Relevant templates	27
Proactive disclosure of personal information by Police	28
Care needed before making proactive disclosure	28
Information Privacy Principle 11	28
Information obtained for the purpose of disclosure (IPP 11(1)(a))	28
Example	28
Maintenance of the law (IPP 11(1)(e)(i))	28
Elements of IPP 11(1)(e)(i)	28
Example	29
Necessary for the conduct of legal proceedings (IPP 11(1)(e)(iv))	29
Example	29
Threats to health and safety (IPP 11(1)(f))	29
Elements of IPP 11(f)	30
Information sharing between agencies (within New Zealand)	31
Permitted sharing of law enforcement information	31
Information sharing agreements (MOU, LOA, etc)	31
Approved Information Sharing Agreements (AISAs)	31
International information sharing	33
Under the Privacy Act	33
Under the Policing Act 2008	33
International information sharing delegations and directions	33
Appendix A: Triage processes for PNHQ and Districts	34
PNHQ Ministerial Services Triage Process	34

Districts Triage Process	34
Appendix B - Withholding information and refusing requests under the Privacy Act	35
Introduction	35
Response	35
Information is not readily retrievable or not held	35
Grounds for refusing requests or withholding information	35
“Would be likely” - meaning	35
Grounds relating to the protection of an individual	35
Seriously threatening safety, etc	35
Creating likelihood of harassment	36
Creating distress to victims	36
Breaching a promise of confidentiality in employment matters	36
Other grounds for refusing access	36
Information does not exist or cannot be found	36
Disclosing the affairs of another person	36
Prejudicing the maintenance of the law	36
Breaching legal professional privilege	37
Refusing because the Criminal Disclosure Act applies	37
Refusing because the request is frivolous or vexatious	37
Classified or confidential information	37
If request relates to current investigation and trial	37
After the trial	37

Note: this is an extensively rewritten policy, published 1 December 2020. Some sections are still undergoing updates.

Introduction

Purpose of this chapter

This part of the '[Privacy and official information](#)' chapter details:

- the purpose of the [Privacy Act 2020](#)
- the three information privacy principles most relevant to Police responses to requests for and disclosure of personal information
- **the law** you must consider before disclosing personal information:
 - **reactively** - in response to Privacy Act requests from individuals seeking information about themselves
 - **proactively** - in the absence of a request for information to third parties (see [Proactive disclosure of personal information by Police](#))
- **the procedures** to be followed when **responding to requests** for personal information using the Information Request Tool (*IRT*). These procedures apply to Privacy Act **requests** received at PNHQ and in Districts. See '[How to action a Privacy Act request - an overview of the processing stages](#)'. (Note that the **IRT is not used** for 'proactive' disclosure of personal information).

This chapter also includes general information on:

- [Information sharing between Police and agencies within New Zealand](#), and
- [International information sharing](#).

See '[Disclosure under the Official Information Act 1982 \(OIA\)](#)' for the legislation and procedures relating to requests for official or non-personal information, or personal information about third parties, under the [Official Information Act 1982](#).

This part of the '[Privacy and official information](#)' chapter also provides detailed Police processes to guide staff when receiving and responding to Privacy Act requests using the Information Request Tool (*IRT*). It applies to all Privacy Act requests received at PNHQ and in Districts. See the section on '[How to action a Privacy Act request](#)'.

Personal information defined

"Personal information" means any information about an identifiable person. ([s7](#))

When does the Privacy Act apply?

The [Privacy Act 2020](#) applies both when responding to a request for personal information about the requester and when proactively disclosing personal information. Requests for official information (which includes personal information about someone who is not the requester) are considered under the [Official Information Act 1982](#) (see '[Disclosure under the Official Information Act 1982 \(OIA\)](#)').

References to 'the Act'

References to sections only or to 'the Act' are to the Privacy Act 2020 unless otherwise stated.

Purpose of the Privacy Act

The Privacy Act 2020 promotes and protects individual privacy by:

- establishing 13 [information privacy principles](#) (IPPs) which:
 - govern the collection, storage, use and disclosure of personal information by agencies (including Police)
 - provide individuals with the right to access information held about them and to request correction if they consider the information held is wrong
- appointing a Privacy Commissioner to regulate privacy protection, including investigating complaints about privacy breaches.

Information privacy principles relevant to disclosure

The three information privacy principles listed in section [22](#) of the Privacy Act most relevant to responding to requests for and disclosure of personal information are:

- **IPP6** covering requests for access by individuals to information held about them (subject to refusal where good reasons exist);
- **IPP7** covering requests for correction of personal information. If Police is not willing to make the correction sought, Police must take reasonable steps to attach a statement of correction provided by the requester to the information;

- **IPP11** putting limits on when an agency may disclose personal information - that is, disclosure must be permitted by an exception to the rule of non-disclosure. It also governs proactive or voluntary disclosures - that is, the release of personal information in the absence of a request - see [Proactive disclosure of personal information by Police](#).

For more information on information privacy principles generally, see 'Privacy and official information - [Information Privacy Principles \(IPPs\)](#)'

Related information

See also these related parts of the '**Privacy and official information**' chapter:

- [Information Privacy Principles \(IPP\)](#)
- [Collection of personal information](#)
- [Introduction to disclosure of information](#)
- [Disclosure under the Official Information Act 1982 \(OIA\)](#)
- [Applying the Criminal Records \(Clean Slate\) Act 2004](#)
- [Community disclosure of offender information](#)
- [Privacy breach management](#)
- [Personal Information Management](#)
- [Criminal disclosure](#) for the law and procedures relating to the disclosure of information to the defence before trials.

Information Request Tool (IRT) Guides

See the [Ministerial Services Intranet page](#) for detailed process guides on how to log and manage Privacy Act requests in the Information Request Tool (IRT), also used for OIA requests.

Other resources

Other helpful guidance and resources, especially in relation to the sharing of information, is available on the Police intranet> Home > Support Service Resources > Security and Privacy including:

- [Information Sharing Guide \(Public Sector Agency\) \(PDF\)](#)
- [Information Sharing Guide: Agencies seeking to determine risks at an address \(PDF\)](#)

See also the [Office of the Privacy Commissioner's](#) website.

Requests for personal information

Who can make a request

Any living individual or their representative - in New Zealand or overseas - is entitled under IPP6 to make a Privacy Act request for access to their own personal information held by Police (s 40).

Identifying the requester

You must satisfy yourself about the identity of the individual making the request before releasing personal information to them. **Note:** this requirement **does not apply** to requests under the OIA (s 57(a)).

Under the Police 'evidence of identity' standard adopted for personal information requests (see '[Evidence of identity](#)' information on the Police website), you must verify a person's identity in person or through a trusted referee, as follows:

Verifying identity in person

If you are satisfied you know the requester making a request in person, then you probably do not need to sight evidence of identity.

If you do not know the requester, then to verify identity in person, sight a primary and secondary form of identification, one of which must be photographic.

Primary and secondary IDs

Primary ID:	Secondary ID:
<ul style="list-style-type: none"> - original birth certificate - passport - firearms licence 	<ul style="list-style-type: none"> - driver licence - community services card - 18+ card - student/employee ID - credit card - other identification bearing the requester's signature

Verifying identity via a trusted referee

For postal, email or online requests, you can accept either

1. a clear photograph of the requester holding their identification documents (as above); or
2. photocopies of the identification documents (as above) provided the photographic copy has been endorsed as a true copy of the original by a trusted referee who must:

- be over 16, have known the requester for at least 12 months, and not be related or a partner/spouse or a co-resident of the requester

or

- be a person of standing in the community such as a registered professional, religious or community leader, including:
 - Police constable
 - Justice of the Peace
 - Solicitor
 - Registrar or Deputy Registrar of a court
 - Judge
 - other person authorised to take statutory declarations

and

- provide their signature, name and contact details.

Keep a record, including copies, of how you have verified the requester's identity.

Requests for correction of personal information

A person is entitled under IPP7 to request Police to correct the personal information held about him or her, or to attach a statement of correction to the information.

If the information alleged to be incorrect is factual, e.g. date of birth, address or identity, check the accuracy of the information and, if it is wrong, correct it and advise you have do so to the person who requested the correction and any other person the incorrect information may have been provided to.

If the information alleged to be incorrect is not factual but is Police's version of an event or a matter of opinion or an allegation, e.g. a complainant's allegation or a witness' assessment about an alleged offender, do not make the correction. Following appropriate consultation, advise the requester that Police is not willing to alter the information held but that they are entitled to submit a statement of the correction sought.

If the requester supplies a statement of correction, attach it to the file or NIA record so that it will always be read with the disputed information, and advise the requester accordingly. Advise any other people or agencies that received the requester's information of the statement. (s [58-64](#))

IPP6 and IPP7 do not apply to certain information

A person is not entitled to access certain personal information about them under IPP6 or IPP7. This includes personal information contained in:

- correspondence with the Ombudsman or Privacy Commissioner;
- government or public inquiries
- a **video record** made under the Evidence Regulations 2007 or any copy or **transcript** of the video record (s29)

Form of the request

Privacy Act requests can be made in writing or orally. You cannot require that the request be written, but you can ask the requester to put their request in writing. Offer the relevant Police Form (Police Forms>Information Requests> Official Information and Privacy Act Requests> Forms) which can be printed and handed to the requester, or you can direct the requester to the [Police website portal](#) to download/complete/print or to make a request for personal information online.

Otherwise, make a written record of an oral request for personal information, including the full name, date of birth, date and exact wording of request, and how identification is verified.

You must assist a requester so that their request is made in the correct manner or to the appropriate agency. (s[42](#), [61](#))

Time limits for responding to requests

A request must be processed and a decision made on whether and how to grant it, and the requester notified accordingly, as soon as reasonably practicable but not later than 20 working days from the day after the request is received (s[44](#), [63](#), [64](#)). Failing to respond to a request within the time limit or undue delay in making the information available is deemed to be a refusal of the request (s[69](#)(4)&(5)).

Extension of time limit

If you cannot communicate the decision about the request within the 20-working day limit, consider whether you can notify an extension. (s[48](#), [65](#))

Key roles and responsibilities

Oversight at PNHQ

The **Ministerial Services Team** has limited oversight of PNHQ Privacy Act requests. The team receives and triages all Privacy Act requests for completion at PNHQ. It also reassigns Privacy Act requests that need to be completed in districts.

A member of the Ministerial Services Team is designated as the **Ministerial Services Liaison** for each Privacy Act request. The Ministerial Services Liaison logs and assigns requests to the appropriate business group for response directly to the requester. The Ministerial Services Liaison will assist on request in relation to coordinating the response, sending responses to requesters once they are ready, and completing the IRT entry.

End-to-end oversight in Districts

The **Claim Team** (usually those staff in the File Management Centre (FMC) with responsibility for managing information requests) has end-to-end oversight of all Privacy Act requests in the district. A designated Claim Team member (usually the FMC supervisor) is responsible for triaging all Privacy Act requests received. Requests are then allocated to a Claim Team member (this may be the same person) who logs and assigns requests to the **Assignee Team**, then on to a nominated Assignee for response, or reassigns those that need to be completed by another district or PNHQ. The Claim Team maintains oversight of requests to ensure legislative timeframes are met and provides advice to district staff on responding to requests. The Claim Team member is responsible for sending responses to requesters once they are complete.

Preparing the response

A number of people may be involved in the process of preparing a response to a Privacy Act request.

At PNHQ

A **Claim Team** in each business group at PNHQ is responsible for allocating Privacy Act requests received by the business group to an Assignee. The Claim Team maintains oversight of all Privacy Act requests assigned to the business group to ensure they are completed within legislative timeframes.

The **Assignee** is responsible for scoping the request, collating the requested information, and compiling the response for endorsement. The Assignee will usually decide it is appropriate for a **Supervisor** to review a draft response, and possibly also the Director. The Assignee may seek advice from a member of the **Legal Team** at any stage, or ask them to review a draft response once the Supervisor has done so.

In Districts

The **Assignee** is responsible for scoping the request, collating the requested information, and compiling the response. The Assignee would normally seek review by a **Supervisor** of a draft response before it is finalised. The Assignee may seek advice from a member of the **Legal Team** at any stage, or ask them to review a draft response once the Supervisor has done so.

How to action a Privacy Act request - an overview of the processing stages

There are distinct stages involved in receiving and responding to Privacy Act requests (i.e. requests for personal information about the requester) in the Information Request Tool.

1. [Logging and triaging](#) a request
2. [Scoping a request](#)
3. [Collating the information](#)
4. [Compiling the response](#)
5. [Finalising the response](#)

In Week 1	By Week 1-2	By Week 1-3	By Week 2-4†
Log	Collate	Compile response	Provide decision or extension by 20th working day
Triage	Assess	Seek supervisor or NM review	Release approved information without delay
Assign	Compile response		
Scope			
Collate			
Transfer			

Key process points

What you need to know

- Personal information may be held by Police in a number of repositories, principally NIA.

A request for personal information does not need to refer to the Privacy Act, can be communicated by any means (including orally or by social media), and can be made to any person in Police.

Key Timeframes

- You must make a decision about whether you will release the information requested and communicate it to the requester 'as soon as reasonably practicable' and no later than 20 working days after the request is received, unless you have extended the time limit for response. The working day count starts the day after a request is received by Police.

- You have 10 working days to transfer a request to another agency and to inform the requester of the transfer.

Remember

- Members of the public have a right to access the information Police holds about them.

- Privacy Act requests are a core part of our business and any employee may need to be involved in Police's response.

- Communicate well with the requester. Privacy Act requests are an opportunity to build the public's trust and confidence in Police

Logging a Privacy Act request

All **PNHQ Privacy Act requests** are received by the **Ministerial Services Team** and a Ministerial Services Liaison is designated to each request. Any requests sent directly to a business group should be emailed to Ministerial.Services@police.govt.nz for logging and assigning.

All **District Privacy Act requests** are received by the **Claim Team**. Any requests received by another group in that district should be sent to the Claim Team for logging and assigning.

Every request (PNHQ and Districts), including those for correction of personal information, must be logged in the Information Request Tool (IRT) as soon as possible after it is received. This is necessary for workflow management and reporting.

Requests that are submitted through the Police website will automatically be logged in the IRT, with some of the information pre-populated into the request record. A member of the Ministerial Services Team in PNHQ, or the District's Claim Team, will check that the information has pre-populated correctly and add any relevant information.

Requests received by any other means (e.g. oral requests) are logged manually in the IRT by the Ministerial Services Liaison designated to that request, or in Districts, by a member of the Claim Team.

Triaging and assigning requests

The **Ministerial Services Team** or the **designated triage person in each District** triage all Privacy Act requests to ensure that the details are correct and that the request belongs first with Police and then with PNHQ or the District. Ministerial Services or the District Claim Team then assigns the request to an appropriate assignee to prepare the response.

Matters to consider during triage

Consider these preliminary matters during triage and update the IRT accordingly:

- Transfer - does the request need to be transferred to another agency? (full or partial)
- Correct district?
- Confirmation of identity
- Is it confidential?
- Is it of high organisational impact?
- Normal/high priority?
- Will the response time need extending?
- Is the request one to correct personal information held?

Transfer - does the request belong with Police or another agency? [by day 10]

When personal information requested is:

- not held by Police but is believed by the person dealing with the request to be held by another agency, or
- held by Police but is believed to be more closely connected with the functions of another agency,

Police must, not later than 10 working days after the day on which the request is received, transfer the request to the other agency, and inform the requester of the transfer. ([s43](#), [62](#))

However, the obligation to transfer the request does not apply if you have good cause to believe the requester does not want the request transferred to another agency. If the request is not transferred for this reason, you must within 10 days inform the requester that the transfer provision applies, the request has not been transferred, and the name of the agency to which it could be transferred. ([s43\(3\)&\(4\)](#), [62\(3\)&\(4\)](#))

During triage:

- identify if Police holds the information or if another agency should respond. If Police doesn't hold the information, or holds only part of it, or the information is more closely connected to the functions or activities of another agency, **transfer the request** (unless you have good cause to believe the requester objects)
- if the information is spread across multiple agencies, Police may need to split the request, respond to part of it, and transfer the remainder to other agencies
- a request that is being transferred in full still needs to be logged in the IRT.

Requests for criminal conviction histories

Do not transfer requests for criminal conviction histories to the Ministry of Justice.

Requests made to Police from individuals for their **formal criminal record** cannot be transferred under the Privacy Act because it is court information held by the Ministry of Justice on behalf of the courts, and courts in relation to their judicial functions are not subject to the Privacy Act. (There has been some misunderstanding and incorrect advice at Police in the past about this relationship.)

The relationship is reinforced in the Privacy Act 2020 in Schedule 4 (Law enforcement information), where Court records have been separated from Ministry of Justice records. Therefore, the Ministry of Justice is no longer designated as the holder of Court information.

People who inquire about getting a copy of their formal criminal record should be referred to the nearest District Court or they can apply on the Ministry of Justice prescribed form. They can obtain the form and further information at <http://www.justice.govt.nz/criminal-records/get-your-own/> or contact the Ministry of Justice by email at criminalrecord@justice.govt.nz.

However, Police can release the **charge history** as held in NIA which includes all Court outcomes, including convictions, especially where it forms part of Police's response to a request for a person's NIA record. Suppressed, Youth Court or clean-slated information may be released under the Privacy Act to the individual concerned as it does not constitute a breach of any order or statutory prohibition on publication.

If the charge history is released, clarify to the requester that it is not the formal criminal record and that, if they want that, they must apply to the Ministry of Justice on the prescribed form (as detailed above).

Is the correct District handling the request?

A District Claim Team is responsible for sending the request to the correct District if the request doesn't belong to them. Ensure the request is entered into the IRT before sending it. (If it came through the public website, it should have already been entered).

Confirm the requester's identity

Confirmation of identity is mandatory for Privacy Act requests. No response is to be provided to the requester without identification being confirmed first (but processing must continue in the meantime).

For **PNHQ Privacy Act requests**, Ministerial Services are responsible at the logging/triage stage for checking that sufficient information has been provided by the requester to confirm their identity. In **Districts**, it is the Claim Team and/or assignee's responsibility to confirm the requester's identity. For more information see 'Confirmation of Identity' in the PNHQ and District IRT Privacy Guides (accessed from the Police Intranet > [Ministerial Services](#) pages).

Is the request confidential?

When triaging, check whether the request should be marked as confidential or not. Marking it as confidential means that only the persons who logged the request or worked directly on responding to it will be able to access it, both while it is active and after it has been closed. (For more information see 'Mark as Confidential' in the PNHQ and District IRT Privacy Guides).

Is there a high organisational impact?

Consider whether it is a 'high organisational impact' request or not. (See [Appendix D in the Disclosure under the Official Information Act 1982 \(OIA\) chapter](#) for examples of requests that may have 'high organisational impact'). Marking it as having high organisational impact in the IRT can help ensure the response receives the appropriate consultation and approvals.

Timeframes and extensions

If a request for access to personal information is not transferred, you must provide Police's response to the request as soon as reasonably practicable and not later than 20 working days after receipt. ([s44\(1\)](#))

Urgent requests

If the requester wants the request dealt with urgently, they must give reasons for this. You must consider the request for urgency and, if reasonable, prioritise it for early response, if practicable. Mark it as 'high priority' in the IRT. ([s41](#), [60](#))

Are there likely to be problems reaching a decision on the response within 20 working days?

To ensure you meet the statutory timeframe for response, you need to:

- Assess the likelihood of the request taking longer than 20 working days to respond to.
- If it is likely to take longer, make sure the assignee is made aware of the process of notifying a time extension.

Extensions - when you can extend the time to respond to a request?

The 20-working day limit for responding can be extended where:

- the request is for a large quantity of information or requires searching through a large quantity of information, and meeting the limit would unreasonably interfere with Police operations, or
- consultations on the decision are required and, as a result, a proper response cannot reasonably be made within the original time limit, or
- processing the request raises issues of such complexity that a response to the request cannot reasonably be given within the original time limit.

The extension period must be reasonable in the circumstances and be notified to the requester before the original time limit expires. ([s48](#), [65](#))

How to notify an extension

Notify the requester of:

- the period of the extension (a good rule of thumb is a further 20 working days, but longer if necessary)
- the reasons for it
- their right to complain to the Privacy Commissioner about the extension (s70)
- any other relevant information.

Acknowledge the request

The Ministerial Services Liaison or the District's Claim Team member needs to:

- Email the requester acknowledging receipt of their request within 24 hours
- Include in the acknowledgement email/letter:
 - the date the request was received by Police
 - the IRT reference number
 - the exact request phrasing of the request, or a copy of the request
 - the timeframe for response
 - if appropriate, address identification deficiencies, notify an extension or transfer.

Assigning Privacy Act requests and accepting responsibility

The same procedures outlined for PNHQ and Districts in the [Disclosure under the Official Information Act 1982 \(OIA\)](#) chapter for assigning and accepting responsibility for OIA requests in the IRT apply to Privacy Act requests. See '[Assigning a request](#)' in the 'Logging and triaging a request' OIA topic. Things to note:

- when assigning to an Assignee Team, consider factors such as subject matter expertise and workload
- consider whether to assign the request to the O/C case or just consult them (for active files or specific records) or to the O/C File Management Centre for coordination of response (including records from multiple districts)
- if the request is for correction of personal information, assign the request to the person who dealt with the original information request (see also '[Responding to requests for correction of personal information](#)' in '[Compiling the response](#)')
- once assigned, the PNHQ or District's Assignee needs to accept or reject responsibility for responding to the request as soon as possible, and within 24 hours (you should talk to the Claim Team member who assigned the response, or your supervisor, before rejecting a request)
- if a Claim Team member or an Assignee identifies that a request, or part of it, needs to be transferred, they should mark the request "for transfer" in the IRT. The Ministerial Services Liaison or the District's Claim Team member will then process the transfer.

Privacy Act template letters

- Acknowledgement letter (or email)
- Letter to agency - transfer of request
- Letter to requester - transfer of request
- Letter to requester - extension

(Accessed from WORD> Police Forms> Information Requests> Official Information and Privacy Act requests)

Checklist for logging and triaging a request [by day 3]

- Request has been logged in the IRT
- Request was assessed for transfer and transfer was completed if required
- Requester's identity has been confirmed
- Request was assessed for confidentiality requirements
- Request was assessed for any high organisational impacts
- Request was assessed for urgency
- Request was assessed for likelihood of any problems reaching a decision on the response within 20 working days
- Requester has been sent an email acknowledging receipt of the request
- Request has been assigned to an Assignee for response

Scoping the information

On accepting responsibility for responding to a request, the next step is for the Assignee to scope the request.

Clarify the request [by day 7]

If the request is not clear enough for the information requested to be identified, contact the requester to clarify their request or give more details. If you clarify by phone and the request is amended, follow up with an email (or letter) to confirm any agreed amendments.

Check for previously released information to the requester

Search the IRT to see if the requester has made previous Privacy Act requests covering the same information, or made the same request to multiple places in Police. If the latter is the case, the response should be completed by the PNHQ business group or district that the majority of the requested information relates to. Notify the requester that they will receive one response and from whom.

Plan your timeline

- A Privacy Act request must be processed and a decision made on whether and how to grant it, and the requester notified, **as soon as reasonably practicable**, and not later than **20 working days** from the day after the request is received.
- You don't have to provide the information that you are releasing to the requester within that timeframe. This does not mean you can defer the decision process; it only applies to the administrative process of providing the information - e.g. applying redactions, but not deciding what to redact. You must still provide the information without undue delay after making the decision.
- Advise the requester when they can expect to receive the information.
- If you cannot communicate the decision within the 20 working day limit, you will need to notify an extension.
- Be realistic when you plan how long each processing stage is likely to take. Keep legislative and administrative deadlines in mind, and consider factors likely to impact how long you need for each stage (e.g. quantity, location and complexity of data, and the number and availability of subject matter experts and other stakeholders).
- Consider your own workload.

Identify who you need input from and who to consult

- This could include the officer in charge of a case or subject matter experts who hold the information or need to be consulted, and internal/external stakeholders/agencies who might need to be consulted or notified.

Identify whether the information exists, its location, how much there is likely to be, and how long it will take to get/assess it

- Does the request require you to create new information? The Privacy Act applies to information 'held' and does not require an agency to create new information in order to grant a request.
- Are there any difficulties accessing the information? Is it readily able to be retrieved?
- Is there likely to be a large quantity of information found, or are you going to have to search through a large quantity of information to find the information that the requester wants?

Identify any risks or impacts with the type of information requested

- The request will have been assessed for any risk or organisational impact during triage, but consider if any new risks/impacts have emerged since then.

Relevant templates

Letter to requester - extension required

(Accessed from WORD> Police Forms> Information Requests> Official Information and Privacy Act requests)

Checklist for scoping a request

[in week 1]

- Request was assessed for whether its scope was clear, and clarification sought if needed
- Checked previously released information or concurrent requests
- Planned request timeline
- Identified SMEs and stakeholders
- Identified whether the information exists, where it is located, how much there is likely to be, and how long it will take to get/assess it
- Identified any issues that could delay collation, assessment, or consultation
- Identified the format that the information (if released) is to be provided in
- Identified any risks or impacts with the type of information requested

Collating the information

Identify information in scope

- Arrange for a search of all physical and electronic locations within Police that you believe may hold information in scope of the request.
- You aren't required to create new information in order to respond to a Privacy Act request. However, you should consider whether it would be administratively unreasonable to refuse to do so (e.g. the work required to create the information is at a manageable level).
- If you need information from another employee, select the "create SME task" option in the IRT. Be clear about the information you need from them, and when you need it.
- Keep a list of locations you've searched and note this in the IRT. If there are subsequent complaints to the Privacy Commissioner, you can show that a reasonable effort was made to identify the requested information.
- If there is a large number of documents in scope, consider keeping a table/list of the documents, to help keep track of them and the action you are taking against each, e.g. consultation, withholding, refusing. (See 'When to withhold information in response to Privacy Act requests'.

Collect copies of the information in scope

When you identify electronic or hardcopy documents you should make copies of these to add to your electronic/physical document set. (Note - it is risky to store original hardcopy documentation in your Privacy request physical document set, as it could be mistaken for copied documentation and redacted or released to the requester).

Issues that may come up during collation

A response to a request for access to personal information can be one of the following:

1. The personal information about the requester is not readily retrievable
2. No personal information is held by Police
3. Police does hold personal information
 1. and access to it is granted
 2. but access to it is refused
4. Police neither confirms nor denies that it holds personal information about the requester. (s44(2))

Information is not readily retrievable or not held

You must notify the requester in your response if

- Police does not hold their personal information in a way that enables it to be readily retrieved; or
- Police does not hold any personal information about them.

(**Note:** the Privacy Act does not require an agency to create information - e.g. write a report or opinion - in order to grant a request for information.) (s44(2)(a)&(b))

The Privacy Commissioner explains that determining:

...whether information is readily retrievable includes consideration of the amount of time and cost required to retrieve the information, when the information dates from, and the manner in which the relevant information is stored.

A lot of information is technically 'retrievable', but this isn't necessarily the same as being 'readily' retrievable.

Consider whether the work required to find the requested information, or bring it together, would have a significant and unreasonable impact on Police's ability to carry out its other operations (e.g. any mention of the requester's name in any records, emails, etc, outside NIA).

Information does not exist or cannot be found

- If the information requested does not exist or, despite reasonable efforts to locate it, cannot be found, the request should be refused under section 53(a) of the Privacy Act.

If you discover relevant information after having refused the request, contact the Ministerial Services Team or your district Claim Team

to discuss the situation as soon as possible.

Before refusing a request for these administrative reasons, consider:

- whether consulting the requester to narrow the scope of the request would enable the request to be granted (e.g. by reducing the time period or types of documents, or explaining their needs)
- what steps have been taken to locate the information
- whether checks have been made with all people who previously had the file
- whether the information is likely to have been destroyed under the Retention and Destruction Schedule agreed with the Chief Archivist
- whether information held could generate the information requested but was not required to be done for operational purposes, and it would require more than minimal effort or cost to be created (e.g. a transcript of a recording)
- whether Police ever held the information sought.

Also ask the requester if they can clarify their request or give more details that may allow the request's scope to be amended. Sometimes people believe Police hold a file on them, but in reality there never was one.

Record in the IRT how big a job it would be to retrieve the information or what steps were taken to thoroughly search for the information before refusing the request.

Large volumes of information

Just because a request is for a large volume of information does not constitute a ground for refusing requests under the Privacy Act. If a large volume of personal information is identified as within scope and is readily retrievable, consider if the timeframe for responding to the request should be extended. Notify an extension as early as possible and no later than by day 20.

Information requested in the course of criminal proceedings

Requests for personal information under the Privacy Act in the course of criminal proceedings should be refused under section [53\(g\)](#), as the Criminal Disclosure Act applies. For more information see 'If request relates to current investigation and trial' in the 'When to withhold information in response to Privacy Act requests' topic.

Limits on charging for providing personal information

You must not charge people for providing them with their personal information (statutory authorisation to charge under s [67](#) is unlikely ever to be available to Police). (s[66\(3\)](#))

Statutory protection when releasing information in good faith

If information is released in good faith in response to a request, you have statutory protection against civil and criminal proceedings. (s [205](#))

Relevant templates

Letter to requester - extension required

Letter to requester - all information withheld/request refused

(Accessed from WORD> Police Forms> Information Requests> Official Information and Privacy Act requests)

Checklist for collating the information

[by week 1-2]

- Requested copies/list of information from all internal information holders
- Received and/or made copies of information in scope
- Compiled list of locations searched
- Compiled list of all information in scope
- If the information is not readily retrievable, contacted requester to discuss amendment, extension, or refusal, if appropriate

Compiling the response

After collating the information, the Assignee needs to decide on and compile the response.

Consider if any information should be withheld or the request refused

A request for personal information can only be refused or information withheld if a reason for doing so applies. The reasons are set out in sections [49](#) to [53](#) of the Privacy Act.

See Appendix B - [Withholding information and refusing requests under the Privacy Act](#).

Consider how personal information can be made available?

Personal information may be made available by:

- allowing the person to inspect the original document
- providing the person with a hard or electronic copy of the document
- allowing the person to listen to an audio recording or watch a video recording
- providing a written transcript
- giving an excerpt or summary of the contents
- telling the person about its contents.

How has the requester asked for the information?

If the requester asks for information to be provided in a particular way, it must be provided in that way unless doing so would:

- impair efficient Police administration, or
- be contrary to a legal duty of the Police in respect of the document, or
- prejudice the interests protected by the withholding grounds in sections [49](#) to [53](#) of the Privacy Act.

If you are not able to provide the information in the manner requested, you must provide the requester with the reason and, if requested, the grounds for that reason, unless doing so would prejudice the interests referred to above. (s [56](#))

Consulting with others

- If you identify any particular risks or issues as you assess the material (e.g. an active investigation), get early advice from supervisors, officers in charge or business owners, the Legal Team, or other relevant Districts/business groups. They may be able to assist you with advice/information to help with your general approach as well as your decision on whether or not to release particular material.
- If material directly relates to other Districts/business groups or external stakeholders/agencies, consult with them to determine what information they consider should be released or withheld and the reasons for this

Making a decision

- Making a decision on the request means deciding whether you will release the requested information to the requester. You must decide whether to release the information in full, release some information and withhold other information, or not release any of the information (refuse the request).

Compiling the information for release

- Police uses Adobe Acrobat XI Pro to **redact information that is being withheld**.
- If you don't have access to Adobe Acrobat XI Pro, contact the Ministerial Services OIA Team or your district Claim Team for advice, as no other method is acceptable.
- Take a PDF scan of each hardcopy document identified, and save a copy of all electronic document files identified.
- You can find information on how to redact [here](#).
- Save a copy of the marked document with the proposed redactions (red outline around the text you intend to redact).
- Save a second version of this marked document and apply the redactions to the second version, then save that redacted version.
- Save both versions in the IRT.
- Add a watermark to the second PDF version which will be released. Follow the guidance on [adding a watermark](#) in the [Electronic redaction and disclosure](#) chapter
- If you have not added watermarks before, create watermarks you will routinely need for different purposes and save the settings - see the suggestions below. It is preferable to personalise the disclosure to easily track the source of a Police document to the recipient and the IRT reference):

Watermark	Title saved
Disclosed under the Privacy Act 2020 To: Ref: IR-	Privacy Act - personalised
Disclosed under the Privacy Act 2020 Ref: IR-	Privacy Act - generic

Drafting a response letter

Irrespective of how the request was made, respond to the requester in writing.

- There are letter templates available to help you. Remember, these are a guide. You can modify them to suit your request circumstances, and provide additional context in your letter, if it will help the requester to better understand the reasons for your decision.
- Use clear language and be as helpful as possible in explaining the rationale for any decisions to withhold information or refuse a request.
- **If the request for access is granted** in whole or in part, inform the requester in writing of:
 - **their right to request correction** of any information they consider is incorrect,
 - **their right to complain** to the Office of the Privacy Commissioner if they are not satisfied with the decision.
- **If information is withheld or the request refused**, inform the requester in writing of:
 - the fact that information is being withheld or the request refused
 - the reason for the decision to withhold or refuse (i.e. the relevant Privacy Act provisions)
 - the grounds supporting that reason if:
 - the information is evaluative material refused under s 50(1), or
 - disclosure of the grounds is requested by the requester (unless disclosure would prejudice other interests)
 - **their right to complain** to the Office of the Privacy Commissioner if they are not satisfied with the decision
- If you intend to withhold information or refuse a request, consider contacting the requester by phone to explain the decision, before sending the response, if you think this will help Police's relationship with the requester.

Save the response in the IRT, including the information requested - to be released or withheld in full, or proposed and applied redacted versions. **If you consider the unredacted information is not appropriate to be attached in the IRT**, insert its file path location for future reference.

Submit the response to your Claim Team for finalizing.

Reviews

- Decide if your draft response needs review by a Supervisor and/or a member of the Legal Team before it goes:
 - to the Director for approval, if appropriate, or
 - for district requests, back to your district Claim Team to send to the requester
- If a request has been marked as “high organisational impact” in IRT, compulsory reviews or notification may have been identified. Check if this is the case.

Supervisor review

- If you think a Supervisor should review the PNHQ’s draft response, submit a ‘supervisor review’ request in the IRT.

Legal review

- You can ask the Legal Team for advice on withholding grounds for any particular information by submitting a ‘legal review’ request in the IRT.
- If you send a draft response to the Legal Team for review, make sure it has been reviewed by a supervisor first.
- **Be specific** about what parts of the response, or any particular information, you need advice on, and allow adequate time for the Legal Team to respond.

Following completion of any reviews

- Save the response in the IRT, including the information requested - to be released or withheld in full, or proposed and applied redacted versions.
- If you consider the unredacted information is not appropriate to be attached in IRT, insert its file path location for future reference.
- Submit it to your Claim Team for finalizing.

Relevant templates

Letter to requester - extension required

Letter to requester - all information withheld/refused

Letter to requester - some information withheld

Letter to requester - all information provided

(Accessed from WORD> Police Forms> Information Requests> Official Information and Privacy Act requests)

Checklist for compiling the response

[by week 1-3]

- Compiled files or hardcopy documentation for assessment
- Reviewed the withholding/refusal grounds in the Act if needed
- Reviewed each piece of information in scope carefully and assessed it for release
- Sought early advice from Legal Team or other Districts /business groups if needed, particularly if withholding information or refusing any part of request
- Identified stakeholders who need to be advised about the request and/or have the opportunity to consult on the response, and/or receive a copy of the final response prior to release
- Made a decision in respect of each part of the request
- Compiled release copy of requested information (if applicable)
- Drafted response letter
- Completed Supervisor review if needed, and made any necessary amendments
- Completed Legal review if needed, and made any necessary amendments
- Completed all appropriate consultation with stakeholders

Finalising/approvals (PNHQ/Districts)

Approval before release

The Claim Team member needs to consider if:

- any further consultation is required before the response is released
- the response requires approval by a manager before it is sent to the requester. This may be the case for requests that have been marked 'high organisational impact'.

Use a secure method of disclosure

If releasing the requested personal information in hard copy (by hand or by courier), mark it 'private' or 'confidential'; if releasing by email, take great care to ensure the email address is correct. It is advisable to send a prior email to enable the requester to confirm they are expecting to receive it, as emails are often available to other users of a device. It is also highly recommended that you open any attachments to check briefly that it is the redacted version of the information to be released before hitting 'send'.

Releasing the response

When the response is complete, the Claim Team member sends it to the requester.

The Claim Team member needs to:

- Check if the requester has asked for the response to be sent to them in a particular format or by a particular delivery method (e.g. email or post).
- Send the response to the requester (with a prior email and checking attachments, as above, if appropriate).
- Make sure all documents relating to the request and response are saved in the IRT, including:
 - consultation emails
 - the information provided (a replica of what was released)
 - any information that was **withheld** (the marked-up but unredacted version)
 - all correspondence relating to the request
 - a note recording any oral advice received (e.g. legal advice obtained by phone)
 - the response letter or email as sent
- Record in writing what you have done to respond to the request. This becomes important if a subsequent complaint is made to the Privacy Commissioner about Police's response.
- Complete/close the request in the IRT.

Relevant templates

Letter to requester - extension required

Letter to requester - all information withheld/refused

Letter to requester - some information withheld

Letter to requester - all information provided

(Accessed from WORD> Police Forms> Information Requests> Official Information and Privacy Act requests

Checklist for finalising the response

[by week 2-4]

- Considered if the request requires any further review or approval
- Response sent to requester in the format requested
- Saved all documents relating to the request in the IRT
- Completed and closed the IRT record

Proactive disclosure of personal information by Police

(**Note:** Proactive disclosure of personal information is not managed in the Information Request Tool).

Care needed before making proactive disclosure

Disclosing personal information in the absence of a request can constitute an interference with the individual's privacy and lead to civil action. The Human Rights Review Tribunal has the power to award damages of up to \$350,000 in such cases. It is therefore important to think carefully, take guidance and perhaps consult with Police Legal Services before making any proactive disclosure.

Information Privacy Principle 11

Information Privacy Principle (IPP) [11](#) (s 22 Privacy Act 2020) must be applied when deciding whether to disclose information in the absence of a request. This privacy principle prohibits the disclosure of personal information unless you **believe on reasonable grounds** the disclosure is permitted by one of the listed exceptions.

The exceptions most relevant for Police are contained in IPP 11(1)(a), 11(1)(e)(i), 11(1)(e)(iv) and 11(1)(f).

Information obtained for the purpose of disclosure (IPP 11(1)(a))

If the information was obtained specifically to pass on to a third party, or if such onward transmission is directly related to the purpose for which the information was obtained, the disclosure to that third party is sanctioned by IPP [11](#)(1)(a).

Example

One of the purposes Police collect information about the victim and the offender in a family violence incident is to assist the parties involved by disclosing information to another agency that provides support and assistance, e.g. to Women's Refuge or Victim Support. As it was one of the purposes of collection, and the individuals ought to have been told about this purpose, disclosure of information in the family violence reports is permitted by principle 11(1)(a).

Similarly, some information collected during enquiries into air crashes, traffic accidents, or deaths in workplaces may be conveyed to the CAA, LTSA or WorkSafe New Zealand.

Maintenance of the law (IPP 11(1)(e)(i))

Disclosure is permitted where necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, prosecution, and punishment of offences.

There are three key elements of principle [11](#)(1)(e)(i). You must:

- identify a prejudice to the maintenance of the law
- believe on reasonable grounds that such prejudice is likely to occur, and
- believe that disclosure is necessary to avoid the prejudice.

Elements of IPP 11(1)(e)(i)

Element	Explanation
Prejudice to the maintenance of the law	First , identify in what way the maintenance of the law would be prejudiced if the information were not disclosed. For example, an offence may be committed, an investigation may be prolonged or frustrated or a witness may not assist with enquiries.
Reasonable grounds to believe prejudice is likely to occur	Second , you must be able to list facts supporting the probability of the prejudice occurring. For example, if a person charged with a sexual grooming offence is employed in a school, reasonable grounds to believe that offending might occur would include the fact that he has the opportunity to be alone with children of relevant ages.
The disclosure must be necessary	<p>Third, you must believe the prejudice to the maintenance of the law will be created if the disclosure is not made. In effect, this means that:</p> <ul style="list-style-type: none"> - Disclosure must be the last resort. Ask yourself: “Is there any way to prevent the identified prejudice to the maintenance of the law other than by disclosing the information at issue?” If the answer is ‘no’, the disclosure is necessary. Otherwise, it is not. - It must be made only to a person(s) who can prevent the identified prejudice to the maintenance of the law. For example, disclosing to a school principal that one of his staff has been charged with sexual grooming would enable the principal to take steps to review the employment decision or to ensure that the offender does not have unsupervised contact with children or opportunity to re-offend. Advising the parent body would not be necessary to achieve that purpose. - Sufficient information to ensure the identified prejudice is prevented should be disclosed. Superfluous detail should not be disclosed.

Example

An officer made enquiries to locate a person at the address of that person’s parents. She was not home but, in response to her mother’s question, the officer disclosed that the reason for wanting to locate her was to serve a notice under section 30A of the Transport Act 1962 disqualifying her indefinitely from driving. Police was found to have breached the person’s privacy under principle 11 as it was not necessary to tell the offender’s mother.

Necessary for the conduct of legal proceedings (IPP 11(1)(e)(iv))

Personal information may be disclosed to third parties if you have reasonable grounds to believe disclosure is necessary for the conduct of proceedings before any court or tribunal (that have been commenced or are reasonably in contemplation). Legal advice should probably be sought prior to disclosure.

Example

Police has on file evidence that directly conflicts with an affidavit sworn and filed by a party to civil proceedings, and brings the evidence to the court’s attention.

Threats to health and safety (IPP 11(1)(f))

Police will often have reason to rely on this exception to the principle of non-disclosure where necessary to prevent or lessen a serious threat to safety.

There are three key elements of principle 11(1)(f). You must:

- identify a serious threat (as defined - see below) to public health or safety, or to the life or health of at least one individual, and
- believe on reasonable grounds that such threat is likely to occur, and

- believe that disclosure is necessary to prevent or lessen the threat.

Elements of IPP 11(f)

Element	Explanation
Threat to health or safety	<p>First, it is essential to identify a threat to the public or to the health or safety of at least one individual. The threat must be “serious” as defined in section 7(1) - i.e. having regard to</p> <ul style="list-style-type: none"> - the likelihood of the threat being realised; - the severity of the consequences if it is; and - when it might happen. <p>For example, where you believe a person is at risk of harming themselves or someone else, you may be justified in disclosing that to someone who may be able to prevent it.</p>
Reasonable grounds to believe threat will be prevented or lessened	<p>Second, there must be reasonable grounds for believing that disclosure will prevent or lessen the identified threat. For example, if the Police inform the public that a dangerous prisoner has escaped, the public can take precautions to secure their homes and cars and keep their families safe. The fact that people on their guard are less at risk than they would otherwise be provides a reasonable ground for Police to believe that disclosure of the escape would prevent or lessen the threat to the public.</p>
The disclosure must be necessary	<p>Third, the disclosure must be necessary. In effect, this means that:</p> <ul style="list-style-type: none"> - It must be the last resort. Ask yourself: “Is there any way to prevent or alleviate the identified threat other than by disclosing the information?” If the answer is ‘no’, the disclosure is necessary. Otherwise, it is not. - It must be made only to a person(s) who can prevent or lessen the identified threat. - Sufficient information to ensure the identified threat is prevented or lessened should be disclosed. Do not disclose superfluous detail.

Information sharing between agencies (within New Zealand)

Permitted sharing of law enforcement information

Schedule 4 and Part 7, subpart 3 of the Privacy Act 2020 provide a means for Police and other agencies to access and share law enforcement information. The personal records that may be shared, and the agencies who are entitled to receive that information, are specified in Schedule 4 to the Act:

Court records

[Ministry of Justice records](#)

[Police records](#)

[New Zealand Transport Agency records](#)

[Registrar of Motor Vehicles records](#)

[Road User Charges Collector records](#)

[Department of Corrections records](#)

Schedule 4 is used for one-directional, routine, “always on” access to law enforcement information. In the main, it enables Police to access the information needed to carry out law enforcement functions. It is the legal basis for NIA access to Courts, Corrections and driver information.

Information sharing agreements (MOU, LOA, etc)

Police have a number of formal agreements with other agencies within New Zealand on the sharing of information, which may include personal information. These are documented in Memoranda of Understanding (MOU), operational schedules or appendices to MOUs, Letters of Agreement (LOA) and Protocols, for example:

- MOU with New Zealand Customs Service - see Schedule 2 - Sharing information and intelligence
- MOU with Housing New Zealand
- Information sharing guidelines - family harm - for guidance on what family violence information can be shared with other agencies so that the agency receiving it can carry out its role in preventing further instances of family violence
- Alcohol information sharing guidelines - for how to comply with the law and inform a multi-agency approach to reduce alcohol-related harm, enhance public safety, and develop collaborative problem-solving strategies among regulatory agencies.

These agreements vary but matters covered include what information may be shared, the procedures for doing so, and nominated contacts or designated groups within the agency and Police for managing the sharing of information.

Information shared pursuant to sharing agreements is subject to the provisions of the [Privacy Act 2020](#) and the [Official Information Act 1982](#).

Contact Legal Services for guidance about information sharing agreements.

Templates for Memoranda of Understanding (MOUs) and Letters of Agreement (LOAs) are available in Police Forms > Corporate Instruments. See also the associated Instructions for developing agreements and obtaining approval and signing of them in Police Instructions.

Contact the Corporate Instruments Team in the Policy Group at PNHQ for further advice or email Police.Instructions@police.govt.nz

Approved Information Sharing Agreements (AISAs)

Approved Information Sharing Agreements (AISAs) are made under Part 7, subpart 1 of the Privacy Act 2020. They authorise personal information to be shared to facilitate a public service specified in the AISA. With some exceptions, AISAs can modify or override the Privacy Act’s information privacy principles or codes of practice, or merely clarify the legal basis for information sharing in particular contexts. AISAs have the status of regulations.

AISAs are created when an information sharing agreement is approved by Order in Council on the recommendation of the Minister

responsible for the AISA's lead agency. The Privacy Commissioner must be consulted before an AISA is approved, may make a submission on the AISA, and require regular reporting on the AISA's operation.

Note: The majority of information sharing agreements between Police and other agencies are made, and will continue to be made, by means of a Memorandum of Understanding, or schedule to a Memorandum of Understanding, because the legal basis for sharing already exists in the Privacy Act.

Contact Legal Services for information about when and how to develop an AISA.

International information sharing

Under the Privacy Act

Principle [11](#) of the Privacy Act may permit information sharing internationally (for example, where it is authorised by the individual concerned, or to prevent a serious threat to safety). In particular, principle 11(1)(e)(i) permits NZ Police to disclose personal information but only where it is necessary for NZ Police's purposes - for example, in relation to cross-border offending or joint operations involving NZ Police.

However, a new information privacy principle has been inserted in the Privacy Act 2020 relating to disclosure of personal information outside New Zealand. It is [principle 12](#).

Before sharing information with a policing or other entity in an overseas country under principle 11, principle 12 requires either authorisation from the individual concerned, or a reasonable belief the country is subject to comparable privacy laws or provides comparable privacy safeguards (by being part of a 'prescribed binding scheme', or subject to privacy laws of a 'prescribed country' specified in regulations, or under an agreement between New Zealand and the other country). Police does not need to comply with the requirements of principle 12 when making a disclosure under principle 11(1)(e) or (f) if it is not reasonably practicable in the circumstances.

IPP12 is overridden, in respect of sharing personal information with overseas agencies with corresponding policing functions, by the following provisions of the Policing Act. Nevertheless, the aim of IPP12 - to ensure that personal information sent overseas is subject to privacy safeguards that are similar to those in New Zealand to ensure adequate protection - should be kept in mind and may call for some care before making a cross-border disclosure for law enforcement purposes.

(Note: if the purpose of disclosing information abroad is not for law enforcement, the requirements of IPP12 apply.)

Under the Policing Act 2008

Disclosing personal information for joint operational purposes or solely to assist an overseas law enforcement agency may be permitted under sections [95A-95F](#) of the Policing Act 2008, which (from 7/11/2015) comprise a new subpart entitled **International policing: information sharing to assist corresponding overseas agency**. The provisions permit disclosure where reasonably necessary for an overseas agency to perform a function in its jurisdiction that NZ Police perform under section [9](#) of the Policing Act.

International information sharing can occur only in accordance with either:

- an international disclosure instrument (for example, government treaty, Interpol constitution, or an agency-to-agency agreement entered into by NZ Police); or
- directions issued by the Commissioner.

International information sharing delegations and directions

Only employees with **delegated authority** may share information with overseas police or other agencies with corresponding functions. See 'Policing Act - international information sharing delegations and directions' which contains both:

- delegations from the Commissioner listing authorised employees; and
- directions from the Commissioner for sharing information outside of an international disclosure instrument.

Appendix A: Triage processes for PNHQ and Districts

Download the relevant triage process map (PDF) below:

PNHQ Ministerial Services Triage Process

These are being developed and will be inserted at a future date.

Districts Triage Process

These are being developed and will be inserted at a future date.

Appendix B - Withholding information and refusing requests under the Privacy Act

Introduction

When you have identified what information has been requested, you must consider whether there are any good reasons why the requester should not access any or all the information requested.

Response

A response to a request for access to personal information can be one of the following:

1. The information held about the requester is not readily retrievable
2. Police does not hold any information e
3. Police does hold information
 1. and access to it is granted
 2. but access to it is refused
4. Police neither confirms nor denies that it holds information about the requester. (s44(2))

Information is not readily retrievable or not held

You must notify the requester in your response if

- Police does not hold their personal information in a way that enables it to be readily retrieved; or
- Police does not hold any personal information about them.

(Note: the Privacy Act does not require an agency to create information - e.g. write a report or opinion - in order to grant a request for information.) (s44(2)(a)&(b))

Grounds for refusing requests or withholding information

Requests for personal information may be refused entirely or in part. The grounds for refusing a request or withholding information are listed in sections 49 to 53 of the Privacy Act 2020.

Information can only be withheld from the requester if police have good reasons to believe that a withholding ground applies. The withholding grounds most relevant to Police follow.

“Would be likely” - meaning

The term “would be likely” in the following topics means there must be a distinct or significant possibility of the harm occurring.

Grounds relating to the protection of an individual

New refusal grounds have been added to the Privacy Act 2020 to better cater for situations in which releasing personal information can have a negative effect on someone else.

Police can now refuse to disclose personal information if releasing it would:

- create a serious threat to the health, safety or life of an individual, or to public health or safety (s49(1)(a)(i))
- create a significant likelihood of serious harassment to an individual, (s 49(1)(a)(ii))
- cause significant distress to a victim of an offence, (s49(1)(a)(iii))

The new refusal grounds each have a high threshold before they apply, but they provide Police with the means to find a balance in releasing information when there are other important interests at stake. You may need to consult others (such as the officer in charge or staff involved) as part of your assessment.

Seriously threatening safety, etc

Do not disclose information that would be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety. (s49(1)(a)(i))

The definition of ‘serious threat’ is set out in [s7](#) of the Privacy Act.

The safety risk might relate to the individual concerned, employees, families or other people. There must be a credible reason to believe a threat would be created if the requester receives the information requested.

Creating likelihood of harassment

Do not disclose information that would be likely to create a significant likelihood of serious harassment of an individual. ([s49\(1\)\(a\)\(ii\)](#))

Such behaviour is characterised as repeated, unwanted contact with other individuals in ways that fall short of posing a physical danger to those individuals but that seriously detract from their quality of life. This ground would only apply if there is a significant likelihood of harassment and if the harassment is serious in nature.

Creating distress to victims

Do not disclose information that is about the victim of an offence or alleged offence where disclosure would cause them significant distress, loss of dignity, or injury to feelings. ([s49\(1\)\(a\)\(iii\)](#))

Such behaviour is characterised as repeated, unwanted contact with other individuals in ways that fall short of posing a physical danger to those individuals but that seriously detract from their quality of life. This ground would only apply if there is a significant likelihood of harassment and if the harassment is serious in nature.

Breaching a promise of confidentiality in employment matters

Information which was supplied to Police on a promise of confidentiality in relation to evaluative material compiled to determine suitability for employment or similar purposes may be withheld. Note that the definition of ‘evaluative material’ does not include evaluative or opinion material compiled by a person employed or engaged by Police in the ordinary course of that person’s employment or duties. ([s50](#))

Other grounds for refusing access

Some of the other grounds Police usually rely on to refuse requests or withhold information are in section [53](#).

Information does not exist or cannot be found

If the information requested does not exist or, despite reasonable efforts to locate it, cannot be found, the request should be refused. ([s53\(a\)](#))

Disclosing the affairs of another person

Do not disclose information that involve the unwarranted disclosure of the affairs of another individual or a deceased person. ([s53\(b\)](#))

The right of access under the Privacy Act is limited to personal information about the requester, but sometimes that information is inextricably linked with information about another person. When you have “mixed” information and cannot separate out the information about other people, you have to decide whether releasing the information would involve the unwarranted disclosure of the affairs of another person.

Consider:

- the nature and sensitivity of the information
- the nature of the relationship between the requester and the other person
- the likely reaction of the other person to the disclosure
- the other person’s views about giving access, if known or obtained.

Prejudicing the maintenance of the law

Do not disclose information that would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial. ([s53\(c\)](#))

This withholding ground may apply to a great deal of the information Police holds, but particularly information that:

- is part of an ongoing investigation
- reveals investigative techniques
- identifies an informant, or
- is provided by a witness or complainant who, if disclosed, could deter members of the public from providing information to police in future.

You may need to consult others (such as the officer in charge of an active investigation) as to whether disclosure would **in fact** be likely to cause prejudice to the investigation or a person's right to a fair trial.

See also Classified or confidential information below.

Breaching legal professional privilege

You must withhold information if the request is for a legal opinion or legal advice (s [53\(d\)](#))

Never release communications with Police legal advisers or the Crown without consulting Legal Services.

Refusing because the Criminal Disclosure Act applies

You may refuse a request made by a defendant (or their agent/lawyer) for information that could be sought, or has been disclosed or withheld, under the Criminal Disclosure Act (s[53\(g\)](#))

See If request relates to current investigation and trial below.

Refusing because the request is frivolous or vexatious

You may refuse a request if it is frivolous or vexatious, or the information requested is trivial. (s[53\(h\)](#))

Seek legal advice before relying on this provision.

Classified or confidential information

Classified information cannot be withheld solely on the basis of its security classification or endorsement mark. Urgently refer classified information to the Manager Organisational Security at PNHQ.

The ability to withhold information that someone says is confidential is very limited. Stating that information was provided in confidence is not sufficient to enable it to be withheld on that basis.

A valid withholding ground for classified or confidential information may be based on avoiding prejudice to the maintenance of the law. (s[53\(c\)](#))

If request relates to current investigation and trial

If a request for personal information is made before the commencement of proceedings or does not relate to criminal proceedings, the request is not covered by the Criminal Disclosure Act and the Privacy Act 2020 will apply (including any applicable withholding grounds under the Privacy Act).

Obligations under the [Criminal Disclosure Act 2008](#) begin with the commencement of proceedings and continue until they are concluded.

Any request for information made by a defendant under the Privacy Act in the course of criminal proceedings should be refused under section [53\(g\)](#) as the request is made for information that could be sought, or has been disclosed or withheld, under the Criminal Disclosure Act.

After the trial

The withholding ground in section [53\(g\)](#) does not apply to requests for information relating to the court proceedings made after the trial has concluded. It only applies while criminal proceedings are ongoing and the requester is a defendant.