Disclosure under the Privacy Act 1993

Table of Contents

Executive summary

Key points to note:

The Privacy Act 1993 applies when responding to a request for personal information about the requester and when proactively disclosing personal information.

- Requests from individuals seeking personal information (i.e. information about themselves) must be logged and responded to using the Information Request Database.
- You must give reasonable assistance to the requester, e.g. to enable them to clarify or redirect the request.
- Decisions on requests for personal information must be made and communicated within 20 working days (unless an extension is notified)
- Transfers of requests must be done within 10 working days and extensions notified before the time limit of 20 working days expires.
- Information can only be withheld from the requester if police have good reasons to believe that a withholding ground applies. These grounds are set out in sections 27-29 of the Privacy Act.
- You must follow the procedures in Electronic redaction and disclosure for electronically blanking out information to be withheld to ensure the information cannot be restored or the document modified by the recipient.
- Before disclosing personal information in the absence of a request you must believe on reasonable grounds the disclosure is permitted by one of the exceptions in the Privacy Act, e.g. that the disclosure is necessary to prevent or lessen a serious threat to safety (Information Privacy Principle 11(f)).

Overview

This section contains these topics:

- Purpose of this part
- Personal information defined
- When does the Privacy Act apply?
- Purpose of the Privacy Act
- Information privacy principles relevant to disclosure
- Related information

Purpose of this part

This part of the 'Privacy and official information' chapter details:

- the purpose of the Privacy Act 1993
- 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 (see Proactive disclosure of personal information by Police
- the procedures to be followed when responding to requests for personal information.

Personal information defined

"Personal information" means any information about an identifiable person.
(s**2**)

When does the Privacy Act apply?

The Privacy Act 1993 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)'.

Purpose of the Privacy Act

The Privacy Act 1993 promotes and protects individual privacy by:

- establishing twelve information privacy principles (IPP) 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 to be 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 6 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 voluntary disclosures - that is, the release of personal information in the absence of a request - see Proactive disclosure of personal information by Police.

See 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)
  - 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
- Criminal disclosure for the law and procedures relating to the disclosure of information to the defence before trials.

Other helpful guidance and resources:

Information Sharing Guide (Public Sector Agency)	255.38 KB

Risks at addresses - Information Sharing Guide.pdf	151.19 KB

See also the Office of the Privacy Commissioner's website.

Reactive disclosure - responding to Privacy Act requests

Introduction

When you receive a request from an individual seeking personal information (i.e. information about themselves) you must:

- log the request on the **Information Request Database**
- confirm that the Privacy Act 1993 applies to the request, and give reasonable assistance to the requester (e.g. to enable them to clarify or redirect the request)
- consider preliminary matters (e.g. transfer, extension)
- identify the requester (using the Police Evidence of identity standard)
- action the request
- provide the information requested if there is no reason to withhold it
- even if there is reason to withhold it, respond to the requester within the statutory timeframe.

Who can make a request

A request under the Privacy Act for personal information can be made by any living individual - in New Zealand or overseas. (s34)

Form of the request

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 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. (s38)

How to action a Privacy Act request

Follow this procedure to action the request. This can be done through the O/C of the District File Management Centre or at PNHQ through Executive and Ministerial Services.

Step	Action
1	Make a file for the request (optional), including copies of the request and identification documents. If the request has been made orally, job sheet it or otherwise record it in writing.
2	Log the request on the **Information Requests Database** (IRD) and allocate it to the appropriate business owner. This is the workgroup that holds or is likely to hold the information requested. When the request covers information across a number of workgroups, allocate it to the group responsible for the biggest part of the request and they must then work in consultation with other groups to consider and provide a single response to the request.
3	If a request is allocated to your workgroup but you do not hold the information requested, immediately select the appropriate options in the IRD to reassign or return the request to Ministerial Services or the O/C FMC for re-referral.
4	OPTIONAL: If considered appropriate, enter the request in NIA and code the file 2D. (e.g. if the requester has a NIA identity).
5	Consider the following preliminary matters:

	If the information requested...	**Then...**
	Is not specific enough to enable the information to be identified	Request clarification from the requester immediately.
	Is not held by Police or 'belongs' to another agency	Transfer it within 10 working days (see 'Transferring Privacy Act requests').
	Is so extensive it requires an extension of time for a response (and the requester is not willing to narrow the scope of the request).	Notify an extension (see 'Time limits and extensions')
	Is classified	Urgently consult the Manager Organisational Security at PNHQ. (Classified information must be declassified before it can be released).
	Is held on NIA	Forward the request to the O/C case (for specific records) or to the O/C File Management Centre for coordination of response (including records from multiple districts).
	Is from a Police file currently held by a Crown Solicitor, or relates to a current or past investigation	Forward it to the O/C case of that file for action. (If the O/C case cannot be found, has left Police or is unable to deal with the request, forward it to their supervisor or Area Commander).
6	Draft the response and consider whether the request should be refused, or what can be released and whether any information should be withheld. (See When to withhold information in response to Privacy Act requests). Prepare any material for release in accordance with the procedures in 'Conveying decisions and providing personal information'. Use template letters as a guide, depending on whether none, some or all information is withheld.	
7	Consult with Legal Services if necessary, and any other business groups as appropriate, on the proposed draft and make any changes that are required.	
8	Make and communicate your decision on the request within 20 working days (unless extended).	

Business owners' responsibilities for Privacy Act requests

Business owners of Privacy Act requests are responsible for:

- Determining the scope of information requested and seeking clarification if necessary
- Allocating resources to ensure the request is responded to on time and accurately
- Ensuring that transfers of requests are done within 10 working days
- Ensuring that extensions are notified before time limit of 20 working days expires
- Deciding what information will be released to the requester
- Drafting the response to the request and peer review
- Seeking legal advice about the response if necessary
- Moving the draft response and proposed release of information through the Information Requests Database audit trail within the allocated time frame
- Making any amendments to the draft and/or proposed release or refusal
- Providing the response to the requester by their preferred means
- Retaining a copy of the information considered for release

- Retaining a copy of the information and response sent to the requester on the IRD
- Completing the IRD entry

Privacy Act template letters

Use the template letters as a guide when responding to requests for information under the Privacy Act, including when:

- transferring the request to another agency
- notifying an extension to the time for responding to the request
- responding to the request - depending on whether all, some or none of the information is provided.

See **Information Request Database>Help>Templates & Letters>Letters - Privacy Act templates.**

Identifying the requester

Requester's identity must be verified

You must satisfy yourself about the identity of the individual making the request before releasing personal information to them.
(s45(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:
• original birth certificate • passport • firearms licence	• 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, photocopies of the above identification documents are acceptable 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.

Transferring Privacy Act requests

This section contains these topics:

- When must Privacy Act requests be transferred to other agencies?
- Criminal conviction histories

When must Privacy Act requests be transferred to other agencies?

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 by the person dealing with the request 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.
(s39)

Irrespective of how the request was made, advise the requester in writing (post or email).

For standard letters transferring the request to another agency and informing the requester, see **Information Request Database>Help>Templates & Letters>Letters - Privacy Act templates.**

Criminal conviction histories

A requester will often seek their criminal history. Police does not provide formal criminal conviction histories, which a requester must obtain from the Ministry of Justice.

People who inquire about getting a copy of their criminal record should be referred to the nearest District Court or 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 they can contact the Ministry of Justice by email at criminalrecord@justice.govt.nz.

Requests made to Police from individuals for their criminal record should be transferred under the Privacy Act to:

Criminal Records Unit
Ministry of Justice
SX10161
Wellington

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 their formal criminal record, they must apply to the Ministry of Justice on the prescribed form (as detailed above).

Time limits and extensions

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.
(s40)

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.
(s66(3)&(4)).

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.

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 amount 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.

The extension period must be reasonable in the circumstances and be notified to the requester before the 20-working day limit expires.
(s41)

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 (s67)
- any other relevant information.

For a standard letter notifying an extension, see **Information Request Database>Help>Templates & Letters>Letters - Privacy Act templates.**

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 reasonably practicable, do your best to respond with urgency.
(s37)

When to withhold information in response to Privacy Act requests

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.

Grounds for withholding information

Requests for personal information may be refused entirely or in part. The grounds for withholding information are listed in sections 27 to 29 of the Privacy Act 1993.

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.

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.
(s27(1)(c))

This withholding ground applies 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.

Endangering the safety of any person

Do not disclose information that would be likely to endanger the safety of any individual.
(s27(1)(d))

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

Disclosing the affairs of another person

Do not disclose information that would be likely to involve the unwarranted disclosure of the affairs of another individual or of a deceased individual.
(s29(1)(a))

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.

Information is not readily retrievable, does not exist or cannot be found

If the information requested is not readily retrievable, does not exist or cannot be found, you may refuse the request. (s29(2)(a) & (b))

Record 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.

You must consider:

- what steps have been taken to locate the information
- whether the file has been traced
- whether checks have been made with all people who previously had the file
- whether the information is likely to have been destroyed
- whether Police ever held the information sought.

Also ask the requester if they can clarify their request or give more details. Sometimes people believe Police hold a file on them, but in reality there never was one.

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.
(s29(1)(b))

Other withholding grounds

You can also withhold information if:

- the request is for a legal opinion or legal advice (s29(1)(f)) - never release communications with Police legal advisers or the Crown without consulting Legal Services
- the request is made by a defendant for information that could be sought, or has been disclosed or withheld, under the Criminal Disclosure Act (s29(1)(ia)) - see If request relates to current investigation and trial below)
- the information requested is not held by Police and you have no grounds for believing it is held by another agency or connected more closely with the functions or activities of another agency (s29(2)(c)) - you do not need to create information in order to meet a request
- the request is frivolous or vexatious, or the information requested is trivial (s29(1)(j).

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 is found in section 27(1)(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 1993 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 29(1)(ia) 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 29(1)(ia) 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.

Conveying decisions and providing personal information

This section contains these topics:

- Sending Police's response to the request
- What to tell the requester when information is withheld
- Redacting information that is withheld
- How can personal information be made available?
- Information requested in a particular way
- Use a secure method of disclosure
- Limits on charging for providing personal information
- Statutory protection when releasing information in good faith

Sending Police's response to the request

After considering the information within the scope of the request, you must respond to the requester by deciding to provide it, to withhold it, or to provide some of it. (see When to withhold information in response to Privacy Act requests). When responding, follow these steps.

Step	Action
1	Use template letters as a guide for responding to a request for personal information when nothing is withheld or when some or all information is withheld. (Available on the **Information Request Database>Help>Templates & Letters>Letters - Privacy Act templates.**). Irrespective of how the request was made, inform the requester in writing.
2	If information is withheld, inform the requester in writing of: • the fact that information is being withheld • the grounds on which the decision to withhold has been made • their right to request correction of any information they consider is incorrect, and to complain to the Office of the Privacy Commissioner if they are not satisfied with the decision.
3	Provide the information in the way specified by the requester; otherwise, as photocopies or electronically. Follow the procedures in 'Electronic redaction and disclosure' (part of the Information Management, Privacy and Assurance chapter) for redacting information being withheld and for the secure delivery/release of redacted files. Mark envelopes 'Private & Confidential' and test email addresses before attaching personal information.
4	Keep electronic copies of: • 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.
5	Record in writing what you have done to respond to the request. This process becomes important if a subsequent complaint is made to the Privacy Commissioner about Police's response.

What to tell the requester when information is withheld

If any information sought is withheld, inform the requester of:

- the fact that information is being withheld
- the grounds on which the decision to withhold has been made
- their right to complain to the Privacy Commissioner if they are not satisfied with the decision.

Redacting information that is withheld

Follow the procedures in Electronic redaction and disclosure (Part 10 of the Information Management, Privacy and Assurance chapter) for electronically blanking out (redacting) information to be withheld. These procedures ensure the redacted information cannot be restored or the document modified by the recipient.

How can personal information be made available?

Personal information may be made available by:

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

Information requested in a particular way

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 27 to 29 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.
(s42)

Use a secure method of disclosure

While the usual method of releasing the requested personal information is to provide a photocopy (by hand or by courier marked 'private' or 'confidential'), requesters increasingly wish to receive the personal information by email.

Take great care to ensure the email address is correct and do not provide it by email unless specifically requested, even if the request has been made by email. Emails are often available to other users of a device.

Limits on charging for providing personal information

You must **not charge** people for providing them with their personal information, unless this is specifically authorised by statute.
(s35)

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.
(s115)

Requests for correction of personal information

Follow these steps when a request for correction of personal information held by Police is received.

Step	Action
1	Forward it to the person who dealt with the original information request.
2	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 the person who requested the correction and any other person the incorrect information may have been provided to.
3	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. 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.
4	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.

Proactive disclosure of personal information by Police

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 $200,000 in such cases. It is therefore important to think carefully, take guidance and perhaps consult with the Police Legal Services before making any proactive disclosure.

Information Privacy Principle 11

Information Privacy Principle (IPP) 11 (s6 Privacy Act 1993) 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(a), 11(e)(i), 11(e)(iv) and 11(f).

Information obtained for the purpose of disclosure (IPP 11(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(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, disclosure of information in the family violence reports is permitted by principle 11(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(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(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(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 will be committed, an investigation will be prolonged or frustrated or a witness will not assist with enquiries.
Reasonable grounds to believe prejudice will occur	**Second**, you must be able to list facts supporting the probability of the prejudice occurring. For example, if a convicted sex offender has been employed in a school, reasonable grounds to believe he will re-offend may include the fact that: • he has a series of sex convictions, particularly recent ones • his previous offending occurred in a school environment • there have been reports of him handing out lollies to children or offering them rides home • he did not successfully complete any rehabilitation programmes in prison and has not acknowledged his wrongdoing • he has the opportunity to be alone with children and therefore has the opportunity to offend.
The disclosure must be necessary	**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: • 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 is a convicted sex offender 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. • Only 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(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. This includes proceedings that have been commenced or are reasonably in contemplation.

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(f))

Police will often 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(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	**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 2(1) - i.e. having regard to • the likelihood of the threat being realised; • the severity of the consequences if it is; and • when it might happen. For example, where you believe a person is at risk of harming themselves, you may be justified in disclosing that to someone who may be able to prevent it.
Reasonable grounds to believe threat will be prevented or lessened	**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.
The disclosure must be necessary	**Third**, the disclosure must be necessary. In effect, this means that: • 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. • Only 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 5 and Part 11 of the Privacy Act 1993 provide a means for Police and other agencies to access and share law enforcement information for law enforcement purposes. The personal records that may be shared, and the agencies who are entitled to receive that information, are specified in Schedule 5 to the Act:

- Ministry of Justice records
- Police records
- New Zealand Transport Agency records
- Registrar of Motor Vehicles records
- Ministry of Transport records
- Department of Corrections records

Schedule 5 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
- MOU with IRD - Information sharing schedule
- Information sharing guidelines - family violence - 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 1993 and the Official Information Act 1982.

Contact Legal Services for guidance about information sharing agreements.

Templates for MOUs and LOAs

Templates for Memoranda of Understanding (MOUs) and Letters of Agreement (LOAs) are available in Police Forms>Corporate Instruments. See also the associated 'Instruction' (see PDF below) 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 9A of the Privacy Act 1993. 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(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.

Under the Policing Act 2008

Disclosing personal information solely to assist an overseas law enforcement agency may be permitted under sections 95A-95F of the Policing Act 2008, which 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 9of 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' (PDF below) which contains both:

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

Delegation for information sharing under s95 Policing Act.pdf 138.85 KB

Version number: 1

Owner: NM: Legal Services

Publication date: 11/08/2016

Last modified: 02/10/2017

Review date: 11/08/2018

Printed on : 13/03/2020

Printed from : http://tenone.police.govt.nz/pi/disclosure-under-privacy-act-1993