

Schedule 1 to
NZ Police / DIA MOU

The Commissioner of Police and the
Registrar-General, Births, Deaths, and
Marriages and the Secretary for Internal
Affairs

Information Sharing

1. Recitals

This Schedule is made between the Commissioner of Police (“Police”) and the Registrar-General of Births, Deaths, and Marriages (“Registrar-General”) and the Secretary of Internal Affairs (“DIA”), (together “the Parties”) under the Memorandum of Understanding (MoU) between the Parties dated 27th March 2019.

Police is regulated by the Policing Act 2008. Police’s disclosure of information must comply with the Policing Act and the Privacy Act 1993.

The Registrar-General must comply with the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMRR Act) and the Privacy Act 1993.

DIA must comply with the Passports Act 1992 and the Privacy Act 1993.

The Parties are permitted to share information under section 78AB of the BDMRR Act and part 10A of the Privacy Act 1993.

The Parties have accordingly reached the following understanding.

2. Background

In December 2014, a Government Inquiry (Inquiry) was established following the illegal departure from New Zealand of a prisoner on temporary release. He was able to leave New Zealand using a passport issued in his birth name having renewed his passport in prison. His birth name was not consistently known in the Justice Sector as his birth name and DIA had no record of his other assumed identity in the Passport System or of the court conditions that had been imposed. A cross-agency programme investigated options to better manage identity information across the Justice Sector.

In response to the Inquiry, the then Minister of Justice agreed to three Progressive Steps to improve the quality of the information accessed by Police to more accurately identify individuals. The three Progressive Steps are the provision of:

- i. New Zealand Transport Agency driver licence images to Police
- ii. birth, passport, and immigration biographic information and associated images to Police
- iii. registered deaths and name changes information to Police.

Implementation of these steps is expected to reduce the risk of offenders using multiple identities that differ across various Justice Sector agencies and will contribute to the reduction in the number of events relating to misidentified individuals.

The Enhancing Identity Verification and Border Processes Legislation Act 2017 inserted section 78AB into the BDMRR Act to enable specified agencies to receive birth, death, marriage, civil union, and name change information for law enforcement purposes. Police is a ‘specified agency’ under section 78AB(5) of the BDMRR Act.

3. Purpose

This Schedule provides for the sharing of specified information in accordance with section 78AB of the BDMRR Act and part 10A of the Privacy Act 1993. Information sharing supports the purposes outlined in clause 2.6 of the MoU.

This Schedule is made under clause 1.4 of the MoU and is intended to be read in conjunction with the MoU.

4. Objectives

The objectives of this Schedule are to ensure that Police can access information held by the Registrar-General and DIA to verify the identity of specific persons Police are interested in or dealing with for policing purposes and for law enforcement purposes, as authorised by or under law.

The identity information disclosed by the Registrar-General and / or DIA will enable Police to better:

- identify the individuals based on birth and passport records, and passport images;
- assist with determining whether the individuals are New Zealand citizens;
- ensure that Police are aware of birth names when an individual is charged and enters the criminal justice system;
- link multiple identities to one individual (e.g. linking to an existing identity and associated criminal history);
- maintain accurate records by correcting identity information (e.g. to maintain accurate databases and registers or to enforce court orders or to apply for and execute warrants);
- detect and correct false information provided by individuals (e.g. detecting identity fraud or individuals attempting to evade Police).

5. Information to be shared

The following types of information may be requested by Police from DIA under the specific legislative provisions below.

The Parties may develop implementing arrangements as appendices to this Schedule. The implementing arrangements may relate to the types of information to be shared, the operational procedures to be followed and technical arrangements concerning the exchange of information between the Parties under this Schedule. The implementing arrangements shall be subject to the obligations set out in this Schedule and the MoU.

Appendix A to this Schedule details the specific information fields to be disclosed by the Registrar-General to a query made by Police.

Appendix B to this Schedule details the specific information fields to be disclosed by DIA to a query made by Police.

5.1. Sharing Passport Information under part 10A of the Privacy Act 1993

Police may request personal information held by DIA on an individual to verify the identity of a person:

- whose identifying particulars have been taken under section 32 or 33 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

The identity information Police may request from DIA is any information that identifies, or relates to the identity of, the individual, and includes (without limitations) the following information:

- 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—
 - New Zealand travel document; or
 - certificate of identity;
- details of any distinguishing features (including tattoos and birthmarks).

5.2. Sharing Birth Information 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.

A non-disclosure direction does not prevent the Registrar-General sharing the above information under section 78AB of the BDMRR Act.

6. How the information will be used

Police will use the information provided by DIA under part 10A of the Privacy Act 1993 to verify the identity of an individual in accordance with the provisions of part 10A.

Police will use the information provided by the Registrar-General under section 78AB of the BDMRR Act for the purposes of law enforcement when requested in accordance with the provisions of that section.

Information received by Police from the Secretary Internal Affairs or the Registrar-General may be used to correct and update records held by Police, but will not otherwise be retained.

The Parties will ensure that information shared under this Schedule will only be used and accessed by appropriately trained, qualified and authorised staff.

7. Disclosure to third parties

Nothing in this Schedule is intended to affect the ability of the Parties to exchange or access information pursuant to any other information sharing agreement or enactment, including the ability to access identity information pursuant to the Privacy Act 1993.

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.

8. Procedure for sharing information

Information may be exchanged between the Parties by various means including:

- by other technological means, including direct access to the information via an Application Programming Interface (“API”); or
- on an ad-hoc basis, including exchange via telephone or via secure email.

The detailed process for sharing information under this Schedule is described in Appendices A and B.

Information is provided by Parties on a best endeavours basis. There is no guarantee of system availability.

9. Safeguards to protect personal information and minimise privacy risks

Police will comply with applicable legislation, including ensuring that personal information is only accessed and used:

- by persons acting in the course of their official duties as employees of Police, and
- in accordance with any specific purposes for accessing information under section 78AB of the BDMRR Act and part 10A of the Privacy Act 1993.

Police will ensure that all personal information received from DIA is protected by reasonable security safeguards against loss, unauthorised access, use, modification, or disclosure, or any other misuse.

The following safeguards exist to protect the privacy of individuals and ensure that any interference with their privacy is minimised:

- The Parties, including their staff, will abide by the Public Sector Standards of Integrity and Conduct, and specifically for Police staff, the Police Code of Conduct.
- Information to be transferred to Police under this Schedule will be extracted from the appropriate system based on a pre-defined query.
- The information to be transferred to Police under this Schedule will be transferred securely to Police in accordance with the requirements of the New Zealand Information Security Manual (NZISM).
- Access to the National Intelligence Application (NIA) is role-based and managed by Police's information security and user access policies. NIA is a secure database, accessed by users through a Police account.
- Police staff are trained in the use of NIA.
- Police's Professional Conduct unit regularly audits usage through transaction logs and has committed to doing the same for DIA queries.
- NIA is protected by several layers of security, including firewalls and intrusion detection and subject to regular testing.

10. Retention and disposal

Both Parties shall ensure that any information shared is stored and managed in accordance with mandated security policies, including the Parties' privacy, data and information retention, and security policies, practices and procedures.

The Parties will comply with any Government security protocols regarding storage, retention and destruction of information.

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

Information received under this Schedule will be stored by each Party in a secure system that protects the information against unauthorised use, modification, destruction, access and disclosure or any other misuse.

Information shared under this Schedule 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.

11. Fees/costs

Fees associated with this Schedule, if any, will be agreed by the Parties.

12. Security and privacy provisions

If any Party has reasonable cause to believe that any breach of any security or privacy provisions in this Schedule has occurred, or may occur, that Party may undertake investigations in relation to that actual or suspected breach as is deemed

necessary. Where an internal investigation confirms a security or privacy breach the other Parties will be notified as soon as possible.

Where an internal investigation confirms the loss of, or unauthorised access to, personal information amounting to a significant privacy breach, the Privacy Commissioner will be notified as soon as possible. The parties will observe any legal requirements to notify the Privacy Commissioner or individuals of privacy breaches.

The Parties will take all reasonably practicable measures to mitigate and remedy the effects of any such breach.

All Parties shall ensure that reasonable assistance is provided to the investigating party in connection with all inspections and investigations. The investigating Party will ensure that the other Parties are kept informed of any developments in the investigation.

Any Party may suspend the information sharing process to allow time for a security or privacy breach to be remedied.

13. Dispute resolution

Should any dispute or difference relating to the application or interpretation of this Schedule arise, the Parties will meet in good faith with a view to resolving the dispute or difference as quickly as possible.

Where there is any dispute between the Parties, the matter shall initially be referred to the District Manager: Criminal Investigations of the Police District where the information was exchanged or sought, and to the Manager Information Partnerships, Te Pou Manawa, Service Delivery and Operations for the Department of Internal Affairs.

Matters that remain unresolved or need further adjudication, will be referred to Police National Manager: Criminal Investigations or General Manager, Te Pou Manawa, Service Delivery and Operations for the Department of Internal Affairs. If agreement cannot be reached within 28 days of the referral, the matter will be referred, in writing, to the Registrar-General Births, Deaths, Marriages, the Secretary of Internal Affairs and the Commissioner of Police for final resolution.

The Parties shall continue to comply with their obligations under this Schedule despite the existence of any dispute or difference.

14. Review of Schedule and reporting

The Schedule will be reviewed by Parties 12 months after its signing.

Further reviews will be undertaken as part of a review of the MoU.

Each Party must report annually on the details of the operation of sharing in this Schedule in accordance with section 78AB of the BDMRR Act and part 10A of the Privacy Act 1993.

15. Amendments to Schedule

The Parties will enter into consultations with respect to amendment of this Schedule at the written request of any Party.

The Schedule may be amended at any time by the mutual written agreement of the Parties. An amendment to the Schedule commences on the day that all Parties have agreed in writing to the amendment.

16. Quality assurance and audit

The Parties agree to cooperate to allow Police to conduct an audit if requested. Police agree to share the results of any audit with the other Parties. The Police audit, if any, will confirm that the safeguards in the Schedule are operating as intended, that they remain sufficient to protect the privacy of individuals, and to ascertain whether any issues have arisen in practice that need to be resolved.

The Parties agree to assist and support each other with quality assurance and/or audit activities that may arise from time-to-time.

The Parties will consult with each other regarding the scope of assistance and support to be provided to each other.

17. Term and termination

This Schedule commences on the date the last Party signs the Schedule.

The Schedule shall continue in force until terminated by any Party. Any Party may terminate this Schedule without cause by providing three months' written notice to the other Parties.

Any Party may suspend, limit, or terminate this Schedule if it appears to that Party that the terms of the Schedule are not being met or have been breached or the information sharing under this Schedule is otherwise unlawful.

If extraordinary circumstances arise (including but not limited to acts of God, earthquake, eruption, fire, flood, storm or war or industrial action, strike, or lockout) which prevent any Party from performing its obligations under the Schedule, the performance of that Party's obligations shall be suspended for as long as those extraordinary circumstances prevail.

18. Media and information requests

The Parties will consult with each other before responding to any media enquiry relating to this Schedule.

The Parties are responsible for complying with their respective obligations under the Privacy Act 1993, the Official Information Act 1982, and any other applicable legislation.

If any Party receives a disclosure request, including under the Privacy Act 1993 or Official Information Act 1982, that relates to information exchanged under this Schedule, the Party that received the request will consult with the other relevant Parties as soon as practicable regarding the request or where the request for information appears to more closely relate to one Party's functions, the Parties agree that the request will be transferred to that Party in accordance with section 14 of the Official Information Act 1982.

19. Operational contacts

Each Party will appoint a contact person to co-ordinate the operation of this Schedule with the other Parties. The initial contact persons are as follows:

Party	Contact
Police	Tim Anderson National Manager: Criminal Investigations
Registrar-General	Adrian Jarvis Deputy Registrar-General Births, Deaths and Marriages Service Delivery & Operations
Secretary of Internal Affairs	Louise Cole Manager Information Partnerships Te Pou Manawa Service Delivery & Operations

All notices and other communication between the Parties under the Schedule shall be sent to the operational contacts.

The operational contacts may be updated from time to time by notice (which may be sent by email) to the other Parties.

20. Signatories

The Parties' signatories to this schedule are:

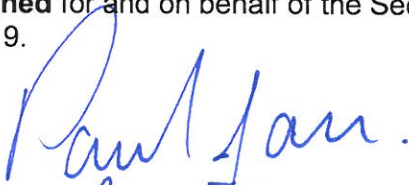
Signed for and on behalf of the Registrar-General, Births, Deaths, and Marriages on the 27th day of March 2019.



Name: Jeff Montgomery

Designation: Registrar-General, Births, Deaths, and Marriages.

Signed for and on behalf of the Secretary of Internal Affairs on the 3rd day of April 2019.



Name:

PAUL JAMER
Designation: Secretary of Internal Affairs

Signed for and on behalf of the Commissioner of Police on the 8th day of April 2019.



Name: Mike Bush MNZM
Designation: Commissioner of Police

Appendix A – Information to be shared between the Registrar-General and Police

1. Information to be shared by Police

Police will provide the following information to the Registrar-General regarding the individual:

- First name(s) (optional)
- Surname
- Date of birth
- Gender

Police will also provide the following information to the Registrar-General regarding the query:

- Requesting Police Officer ID
- Requesting Officer's HR location
- Query reason. This will be one of the following:
 - Query Person – when an Officer queries an individual outside of the custody module.
 - Query Custody – when an Officer queries an individual within the custody module.

2. Matching rules for birth queries

The first name(s) (if provided), surname, date of birth and gender must match for an individual to be considered to be matched.

Conditions for matching the first name(s) are:

- Only one entire name element needs to match for a result to be returned
- The order the names are presented does not matter
- If the name exists in the transliteration list, and one of those names match
- Searches are case-insensitive.

Conditions for matching the surname are:

- All parts of the surname must be present
- These non-alphanumeric characters are ignored ; # ' () , - @ `
- Spaces are ignored
- Searches are case-insensitive
- No transliteration support.

Conditions for matching the date of birth are:

- Dates will be matched
- Times will be ignored.

Conditions for matching the gender are:

- If female is provided by Police then it matches records containing female or indeterminate
- If male is provided by Police then it matches records containing male and indeterminate
- If gender unknown / indeterminate is provided by Police then it matches all records.

3. Information to be shared by the Registrar-General for birth queries

The Registrar-General will disclose the following information from the individual's registered birth record in the event of an identified match:

- Current first name

- Current surname
- Previous first name(s)
- Previous surname(s)
- Previous name(s) effective date(s)
- Surname at birth
- First name(s) at birth
- Gender
- Date of birth
- Place of birth
- Still born indicator
- Death indicator

A matched individual's information will be shared with Police where a non-disclosure direction exists.

4. Information not to be shared by the Registrar-General for birth queries

The following information will not be shared by the Registrar-General:

- Pre adoption registered birth records
- Pre sexual assignment or reassignment birth records
- Records with a Domestic Violence Act 1995 non-disclosure direction in place.

5. Method of information sharing

Information is exchanged via an API. The following apply:

- The information will be encrypted while in transit between the Parties;
- The API will validate queries and search results to ensure their validity; and
- Access to the API will be subject to role-based access controls.

6. Retention

Information received by the Registrar-General from Police may be retained indefinitely.

Information received by Police from the Registrar-General may be used to correct and update records held by Police, but will not otherwise be retained.

Appendix B – Information to be shared between the Secretary of Internal Affairs and Police

1. Information to be shared by Police

Police will provide the following information to the Secretary of Internal Affairs regarding the individual:

- First name(s) (optional)
- Surname
- Date of birth
- Gender

Police will also provide the following information to the Secretary of Internal Affairs regarding the query:

- Thumbnail required indicator
- Requesting Police Officer ID
- Requesting Officer's HR location
- Query reason. This will be one of the following:
 - Query Person – when an Officer queries an individual outside of the custody module.
 - View Details – when an Officer selects a specific item from a result list outside of the custody module.
 - Retrieve – when an Officer requests 'the latest' details for a linked identity or when an Officer selects a specific identity from a result set outside of the custody module.
 - Query Custody – when an Officer queries an individual within the custody module.
 - View Details Custody – when an Officer selects a specific item from a result list inside of the custody module.
 - Retrieve Custody – when an Officer requests 'the latest' details for a linked identity within the custody module.

2. Matching rules

The first name (if provided), surname, date of birth and gender must match for an individual to be considered to be matched.

Conditions for matching the first name are:

- Only one entire name element needs to match for a result to be returned
- The order the names are presented does not matter
- If the name exists in the transliteration list, and one of those names match
- Searches are case-insensitive.

Conditions for matching the surname are:

- All parts of the surname must be present
- These non-alphanumeric characters are ignored ; # ' () , - @ `
- Spaces are ignored
- Searches are case-insensitive
- No transliteration support.

Conditions for matching the date of birth are:

- Dates will be matched
- Times will be ignored.

Conditions for matching the gender are:

- If female is provided by Police then it matches records containing female or indeterminate
- If male is provided by Police then it matches records containing male and indeterminate
- If gender unknown / indeterminate is provided by Police then it matches all records.

3. Information to be shared by the Secretary Internal Affairs for passport queries

The Secretary Internal Affairs will to disclose the following information from the individual's latest issued passport, regardless if still valid, in the event of an identified match:

- Travel Document Number
- Current first name
- Current surname
- Previous first name(s)
- Previous surname(s)
- Surname at birth
- First name at birth
- Photograph (if thumbnail is requested)
- Date of birth
- Gender
- Place of birth
- Country of birth
- Height
- Eye colour
- Residential address
- Travel document status
- Travel document type
- Travel document issue date
- Death indicator

4. Information not to be shared by the Secretary of Internal Affairs

The following information will not be shared by the Secretary of Internal Affairs:

- Pre adoption name records
- Pre sexual assignment or reassignment name records.

5. Method of information sharing

Information is exchanged via an API. The following apply:

- The information will be encrypted while in transit between the Parties;
- The API will validate queries and search results to ensure their validity; and
- Access to the API will be subject to role-based access controls.

6. Retention

Information received by the Secretary Internal Affairs from Police maybe retained indefinitely.

Information received by Police from the Secretary Internal Affairs may be used to correct and update records held by Police, but will not otherwise be retained.