



**Te Tari Taiwhenua
Internal Affairs**

Information Sharing Agreement

Between

Registrar-General

And

New Zealand Police

Relating to

The supply of registered death, registered name change, and non-disclosure direction information to assist New Zealand Police to perform its functions relating to the maintenance of the law.

Pursuant to Part 9A of the Privacy Act 1993 and section 78AA of the Births, Death, Marriages, and Relationships Registration Act 1995.

Contents

Information Sharing Agreement	3
Defined terms	4
Terms	5
1. Objective and purpose of the Agreement	5
2. Public services the Agreement is intended to facilitate	5
3. Types of information to be shared.....	6
4. Exemptions from the privacy principles	7
5. Parties to the Agreement and lead agency.....	7
6. How the parties may use the information	7
7. Adverse actions	7
8. Operational details for sharing	8
9. Safeguards used to protect the personal information and minimise privacy risks	9
10. Verifying information/identity	10
11. Retention and deletion process.....	10
12. Fees/costs	10
13. Security provisions.....	10
14. Staff training.....	10
15. Privacy breaches	11
16. Audit.....	11
17. Complaints process	11
18. Assistance statement	11
19. Dispute resolution.....	11
20. Review of the Agreement	11
21. Amendments to the Agreement	12
22. Term, performance and termination	12
23. Departmental representatives.....	12
24. Accessing the Agreement.....	13

Information Sharing Agreement

The Parties

Registrar-General

And

New Zealand Police (the Police) (acting through the Commissioner of Police)

The Agreement

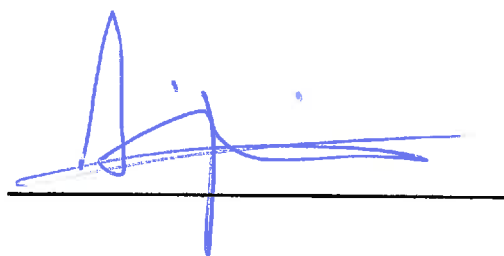
This Agreement is made pursuant to Part 9A of the Privacy Act 1993 and section 78AA of the Births, Deaths, Marriages, and Relationships Registration Act 1995 to enable the Registrar-General to disclose to the Police personal information relating to registered deaths, registered name changes, and non-disclosure direction information. Sharing this information will enable Police to improve the accuracy of the personal information in its national database of identity information and assist the Police to perform its functions relating to the maintenance of the law.

Acceptance

In signing this Agreement, each Party acknowledges that it has read and agrees to be bound by it.

For and on behalf of **Registrar-General**

For and on behalf of **New Zealand Police**



Deputy Registrar-General
Births, Deaths and Marriages

Commissioner of Police
New Zealand Police

Date: 2/9/19

Date: 9. 9. 19 .

Defined terms

Term	Definition
Agreement	This Information Sharing Agreement and any amendments made by the Parties and approved in accordance with section 96V of the Privacy Act 1993.
BDMRRA	Births, Deaths, Marriages, and Relationships Registration Act 1995.
Commissioner	The Commissioner of Police appointed under section 12 of the Policing Act 2008.
DIA	The Department of Internal Affairs.
Match	Personal information supplied by the Registrar-General which corresponds with personal information held by the Police about an individual. "Matches", "Matching" and "Matched" have corresponding meanings.
NIA	National Intelligence Application is a secure Police database that contains identity information on individuals following an event (such as a complaint or investigation), as well as information relating to registers (such as the firearms licence register).
Non-disclosure direction	Has the same meaning as in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995.
Operational Procedures	The agreement between the New Zealand Police and the Registrar-General, which details all the operational and technical aspects of the information sharing.
Personal information	Has the same meaning as in section 2(1) of the Privacy Act 1993.
Police	The New Zealand Police.
Privacy Commissioner	Means the Privacy Commissioner appointed under section 12 of the Privacy Act 1993.
Registrar-General	Means the Registrar-General appointed under section 79(1) of the Births, Deaths, Marriages, and Relationships Registration Act 1995.

Terms

1. Objective and purpose of the Agreement

Objective

The objective of this Agreement is to improve the accuracy of the information held by the Police in its national database of identity information, known as the National Intelligence Application (the NIA), relating to the names, deaths, and non-disclosure directions of individuals so as to assist the Police in performing its functions relating to the maintenance of the law.

Increased accuracy of information in the NIA will enable Police to better:

- link multiple identities to one individual (e.g. linking to an existing identity and associated criminal history)
- maintain accurate records about individuals by correcting identity information (e.g. to maintain accurate databases and registers or enforce court orders or warrants)
- detect and correct false information provided by individuals (e.g. detecting identity fraud or persons attempting to evade Police)
- protect the identity of individuals who have a non-disclosure direction in force in respect of their birth or name change information.

There are significant benefits to Police receiving the information:

- Police will be better able to reduce the risk that offenders escape justice by changing their names.
- Police will be better able to provide services to the public by having accurate information about the people it engages with. Police has contact on a daily basis with members of the public, including providing support and reassurance, dealing with complaints, referring to services, activities relating to crime prevention, as well as engaging with victims and witnesses.
- Having accurate information on a person's name or whether a person has died assists Police to continue to provide these public services.
- Having accurate information on whether a non-disclosure direction is in force enables Police to better manage the use of that person's information.

Purpose

The purpose of this Agreement is to improve the accuracy of personal information held by Police in its principal information system, the NIA, which will assist Police performing its functions relating to the maintenance of the law including enabling the Police to:

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

2. Public services the Agreement is intended to facilitate

The public services that this Agreement is intended to facilitate are the functions of the Police specified in section 9 of the Policing Act 2008, which include but are not limited to:

- keeping the peace
- maintaining public safety
- law enforcement

- crime prevention
- community support and reassurance
- national security
- participation in Police activities outside New Zealand
- emergency management.

In addition, this Agreement is intended to facilitate intervention to prevent or reduce harm to individuals and New Zealand society in general.

3. Types of information to be shared

Information that the Registrar-General will share with the Police will be subsets of the complete information contained within a registered death, registered name change and birth record as specified by the BDMRRA. Four subsets of the information that the Registrar-General collects have been determined to be the minimum identifiers necessary to achieve a successful match, enabling the NIA record to be accurately updated with a deceased status, new name, or presence of a non-disclosure direction. The four subsets are below. The specific fields shared are detailed in the Operational Procedures.

- Subset 1 - Information relating to the individual's death that is maintained by the Registrar-General under the BDMRRA:
 - identifying information including, but not limited to, name, sex, date and place of birth, address, and ethnicity; and
 - information specific to the death, including date and place of death, and age at death; and
 - related information including the number of years the person lived in New Zealand for a person born outside New Zealand.
- Subset 2 - Information relating to the individual's name change, their current birth information and all previous name changes (if any) that is maintained by the Registrar-General under the BDMRRA for a New Zealand-born individual who is the subject of a registered name change or a non-disclosure direction:
 - identifying information including, but not limited to names at birth, former names, new names, date and place of birth, and sex; and
 - information specific to the name change registration including date of registration and address at the time of the name change.
- Subset 3 - Information relating to the individual's name change and all previous name changes (if any) that is maintained by the Registrar-General under the BDMRRA for an overseas-born individual who is the subject of a registered name change or non-disclosure direction contained within the Register of name changes for overseas born applicants:
 - identifying information including, but not limited to names, date and country of birth, and address at time of name change; and
 - information specific to the name change registration including date of registration and address at the time of name change.
- Subset 4 - Information relating to an individual's application for a non-disclosure direction or a withdrawal of an existing non-disclosure direction including the date it came into force, was withdrawn or expired that is maintained by the Registrar-General under the BDMRRA.

The personal information being shared excludes the following birth, name change, and death records:

- pre-adoptive birth registrations; and
- pre-sexual assignment or reassignment birth registrations; and
- birth, name change, or death registrations with a non-disclosure direction under Part 9 of the Family Violence Act 2018.

4. Exemptions from the privacy principles

For the purposes of this Agreement, information privacy principles 2 and 11, which are set out in section 6 of the Privacy Act 1993, are modified as follows:

- **Principle 2: Source of Personal Information**
It is not a breach of information privacy principle 2 for the Police to proactively collect bulk personal information relating to registered deaths, registered name changes, and non-disclosure directions from the Registrar-General for the purpose of this Agreement.
- **Principle 11: Limits on disclosure of personal information**
It is not a breach of information privacy principle 11 for the Registrar-General to disclose bulk personal information relating to registered deaths, registered name changes, and non-disclosure directions to the Police for the purpose of this Agreement.

5. Parties to the Agreement and lead agency

This Agreement is between the Police and the Registrar-General. The Police is the lead agency.

6. How the parties may use the information

The Police will use the personal information provided by the Registrar-General to compare that information with personal information held in the NIA.

Successful matches will be used to update the personal information held in the NIA, as appropriate, with:

- an indicator that the individual is deceased; or
- the individual's new registered name and any registered names that are not held in the NIA; and
- an indicator that the individual has a non-disclosure direction in force.

If an individual has a non-disclosure direction and does not have a record in the NIA then a record will be created in the NIA and the indicator for a non-disclosure direction included.

Information provided by the Registrar-General under this Agreement will be used for no other purpose.

7. Adverse actions

The types of adverse action that the Police can reasonably be expected to take as a result of the sharing of personal information under this Agreement are:

- intervention to prevent crime;
- investigation of offences;
- detainment of a person;
- arrest of a person; or
- prosecution of offences.

The Police may use its range of statutory powers to support the exercise of these actions.

The Parties agree that the Police may dispense with the notice requirement under section 96Q of the Privacy Act 1993 where the sharing of personal information under this Agreement gives the Police reasonable grounds to suspect an offence has been committed or will be committed and the personal information is relevant to the detection, investigation, or prosecution of that offence.

Use by the Police could include the prevention, detection, investigation or provision of evidence of a crime. Much of the Police's early assessment and investigative work is confidential to the Police and advance notification of an adverse action could prejudice the integrity of the investigative process.

The most common use of the information is to provide more accurate information on a person's identity or status so that the Police can manage its records. Where Police action uses personal information shared under this Agreement, it will usually support an investigation, for example by confirming an identity in court, or to assist the Police to enforce the law, such as by enforcing a court order. Where personal information shared under this Agreement directly leads to adverse action, such as where there has been a name change for the purposes of committing fraud or an attempt to evade a border alert, giving notice to the person would prejudice the investigation of that offending.

The Police will comply with all Police policies and guidelines as well as the Solicitor-General's Prosecution Guidelines (Guidelines), before taking any adverse action. These Guidelines assist in determining:

- whether criminal proceedings should be commenced
- what charges should be filed
- whether, if commenced, criminal proceedings should be continued or discontinued.

The Guidelines also provide advice for the conduct of criminal prosecutions and establish standards of conduct and practice expected from those whose duties include conducting prosecutions.

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

8. Operational details for sharing

The ongoing operational processes are as follows:

- a. One of the following to occur:
 - a name change application is received from an individual;
 - A Registrar is notified regarding the death of an individual;
 - a non-disclosure direction application is received from an individual;
 - a request to revoke a non-disclosure direction is received from an individual;
 - an in force non-disclosure direction expires; or
 - a correction is received to an existing registered name change or death.
- b. The Registrar follows procedures in accordance with the BDMRRA to register or update these events.
- c. Upon completion of the registration or update, in bulk on a weekly basis or on a timeframe as otherwise agreed in the Operational Procedures, the Registrar-General will provide to the Police in a secure manner from the registration or approved non-disclosure direction the agreed subset of information specified in clause 3.
- d. The Police will run a match of this information against its current information in the NIA.
- e. In the event of a successful match the person's record in the NIA will be amended to reflect the received information. The only amendments made will be:
 - a new name and any registered name not held within the NIA will be uploaded;
 - the person will be marked as deceased; or
 - an indicator that the individual has a non-disclosure direction in force will be entered or removed.

- f. In the event of an unsuccessful match for a new non-disclosure direction then a new record will be created in the NIA and the indicator for a non-disclosure direction included.
- g. The Police will indicate in the NIA that the information was provided by the Registrar-General.
- h. This updated record will then be accessible to the Police for maintenance of the law.
- i. All information received from the Registrar-General will be securely destroyed by the Police, as soon as reasonably practicable, in accordance with the Operational Procedures, following completion of the matching process.

There will be a one-off exchange of non-disclosure direction information relating to current in force non-disclosures once Operational Procedures are agreed by the Parties. This one-off exchange will enable the Police to run a match of this information against its current information within the NIA and enter an indicator for successfully matched individuals that there is a non-disclosure direction in force or create new records for unsuccessfully matched individuals.

Further details regarding the operational processes are included in the Operational Procedures.

9. Safeguards used to protect the personal information and minimise privacy risks

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

- The Parties to this Agreement will abide by the Public Sector Standards of Integrity and Conduct, and specifically for Police staff, the Police Code of Conduct.
- The Registrar-General collects data on deceased persons from funeral directors, or on rare occasions through other parties known to the deceased. Where collection occurs from a Party known to the deceased, they are advised that the information will be released to the Police and the Police may subsequently disclose it to other parties in accordance with legislation.
- Data on name changes is collected directly from individuals or their guardians. Individuals or their guardians are advised when completing a name change application that the Registrar-General will release their information to the Police and the Police may subsequently disclose it to other parties in accordance with legislation.
- Data on non-disclosure directions is collated directly from individuals or their guardians. Individuals or their guardians are advised when completing a name change application that the Registrar-General will release their information to the Police and the Police may subsequently disclose it to other parties in accordance with legislation.
- The DIA privacy notice specifically outlines the circumstances when and how data will be shared under this agreement as an additional notification to the public.
- Information to be transferred to the Police under this Agreement will be extracted from the appropriate DIA system based on a pre-defined query.
- The information will be subject to quality checking and stored securely within DIA's network prior to transfer.
- The information will be transferred securely to the Police in accordance with the requirements of the New Zealand Information Security Manual (NZISM).
- Access to the information transferred from the Registrar-General will be limited to a small number of Police personnel and the file will be stored securely prior to and during use in accordance with the requirements of the NZISM.
- The Police will verify any matched data from the Registrar-General before the NIA record is amended.
- The file will be securely destroyed following completion of the matching process in accordance with the requirements of the NZISM.

- Access to the NIA is role-based and managed by the Police's information security and user access policies.
- Police staff are trained in the use of the NIA and the Police's Professional Conduct unit regularly audits usage through transaction logs.
- The NIA is protected by several layers of security, including firewalls and intrusion detection and subject to regular testing.

10. Verifying information/identity

The Police will not use the shared information for any purpose other than:

- matching identities;
- updating existing personal records in the NIA for successfully matched identities with either a deceased status indicator, the individual's new registered name and any registered names not held in the NIA, and/or an indicator that the individual has a non-disclosure direction in force; and
- creating a new record in the NIA for unsuccessfully matched identities with a new non-disclosure direction.

The personal information listed in clause 3 will be used in the match. The information will be matched manually by a specialised workgroup in the Police.

Further details regarding these processes are included in the Operational Procedures.

11. Retention and deletion process

Matched information will be used to update the NIA as specified in clause 6.

After information in the NIA has been updated or created, no personal information received from the Registrar-General under this Agreement will be uploaded to other Police systems. All personal information received from the Registrar-General will be destroyed, as soon as reasonably practicable, once the matching process has been completed, within the time period specified in the Operational Procedures.

12. Fees/costs

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

13. Security provisions

If either Party has reasonable cause to believe that any breach of any security provisions in clause 9 of this Agreement has occurred, or may occur, that Party may undertake investigations in relation to that actual or suspected breach as deemed necessary. Where an internal investigation confirms a security breach the other Party will be notified as soon as possible.

Both Parties will 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 Party is kept informed of any developments.

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

14. Staff training

Police employees and anyone engaged by the Police must comply with the Police Code of Conduct and other applicable policies and legislative obligations. The Police Code of Conduct prohibits unauthorised access to, or disclosure of, any matter or information in relation to Police business.

Members of Police who perform the matching process will be trained on the operational process and the details of this Agreement.

15. Privacy breaches

Where personal information is found to have been inappropriately accessed or disclosed, the Police and DIA's internal investigation processes will be applied. Where an internal investigation confirms the loss of, or unauthorised access to, personal information the other Party 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 follow the Privacy Commissioner's data breach guidelines and observe any legal requirements to notify the Privacy Commissioner or individuals of privacy breaches. All relevant Parties shall ensure that reasonable assistance is provided to the investigation. The notifying Party shall ensure the other Party is kept informed of any developments.

16. Audit

The Parties will undertake regular first line assurance and internal audits of the operation of this Agreement to confirm that the safeguards in this Agreement 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.

17. Complaints process

The Police will manage any complaints directed to either Party from individuals concerned about the operation of this Agreement. These complaints will be directed through the existing Police complaint channels and this channel will be promoted through both Police and DIA publications.

18. Assistance statement

The Registrar-General and the Police will provide any reasonable assistance that is necessary in the circumstances to allow the Privacy Commissioner or an individual who wishes to make a complaint about an interference with privacy to determine the agency against which the complaint should be made.

19. Dispute resolution

Should any dispute or differences relating to the interpretation or application of this Agreement arise, the Parties will meet in good faith with a view to resolving the dispute or difference as quickly as possible. If the Parties are unable to resolve any dispute within 60 days, the matter shall be referred to the Commissioner and the Registrar-General for resolution.

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

20. Review of the Agreement

A joint review of this Agreement may be undertaken whenever either Party believes that such a review is necessary.

The lead agency shall conduct a review six months after the date on which this Agreement is approved by an Order in Council under section 96J of the Privacy Act 1993. This review will specifically seek to identify the number of successful matches to ascertain whether more (or less) personal information

is necessary to achieve full accuracy. A report of this review will be provided to the Privacy Commissioner upon completion.

Following this initial review, further reviews will occur at intervals specified by the Privacy Commissioner.

Review reports will be included in the lead agency's annual report. The Parties will co-operate with each other in any review and will take all reasonable actions to make the required resources available.

21. Amendments to the Agreement

Any amendment to this Agreement will be made in accordance with section 96V of the Privacy Act 1993. Amendments must be in writing and signed by the Commissioner and the Registrar-General.

Should the Parties be unable to agree on amendments to this Agreement the matter shall be dealt with in accordance with clause 19 above.

22. Term, performance and termination

This Agreement comes into force on the date specified in the Order in Council made under section 96J of the Privacy Act 1993 approving this Agreement.

The Agreement shall continue in force until either the Commissioner or Registrar-General terminates this Agreement, or the Order in Council is revoked.

Either Party may suspend, limit, or terminate this Agreement if it appears to that Party that the terms of this Agreement or the Order in Council are not being met or the information sharing under this Agreement is otherwise unlawful.

If extraordinary circumstances arise (including but not limited to earthquake, eruption, fire, flood, storm or war) which prevent either Party from performing its obligations under this Agreement, the performance of that Party's obligations is suspended for as long as those extraordinary circumstances prevail.

23. Departmental representatives

Each Party will appoint a contact person to co-ordinate the operation of this Agreement with the other Party and will ensure that the contact person is familiar with the requirements of the Privacy Act 1993 and this Agreement. The initial contact persons are as follows:

Police	Registrar-General
Superintendent Iain Chapman	Logan Fenwick
National Manager	Manager Information Partnerships
Criminal Investigations	Partners and Products
	Service, Delivery & Operations

All notices and other communication between the Parties under this Agreement must be sent to the departmental representatives.

The departmental representatives may be updated from time to time by notice (which may be by email) to the other Party. Both Parties are to ensure that the Privacy Commissioner is informed of changes to the departmental representatives.

24. Accessing the Agreement

This document is available to the public online at www.police.govt.nz and www.dia.govt.nz or at:

Police National Headquarters
180 Molesworth Street
Wellington.