

# Police Policy for External Researchers' Access to Resources, Data or Privileged Information

## Introduction

Functions of the NZ Police (hereinafter Police) as defined by the Policing Act 2008 (NZ) include:

- keeping the peace;
- maintaining public safety;
- law enforcement;
- crime prevention;
- community support and reassurance;
- national security;
- participation in policing activities outside New Zealand;
- emergency management.

Police collect data concerning police activity, police personnel, criminal offending, arrests, reported criminal activity, road traffic crashes, and many specialist areas of interest including firearms licensing and search and rescue activity.

Data are disseminated in many forms, including descriptive reports, fact sheets, data tables, journal articles and datasets, transmitted physically or electronically (e.g. via email). Data are analysed and used to develop reports for operational, strategic, policy, and research purposes.

Where it is the custodian, Police aims to maximise access to datasets while ensuring responsible use to protect individual information. Allowing managed access to datasets is regarded as an important way of increasing the benefit gained from the data collected. Where possible, Police aims to support researchers in undertaking research by facilitating access to Police staff (e.g. as research subjects or subject matter experts) or resource (e.g. information and data). Police datasets are potentially available for statistical purposes to public good researchers working within academic institutions, government agencies and the wider sector, subject to certain conditions.

Good statistical practice and our ethical obligations to survey participants and individuals requires that information collected through Police activities, particularly personal information that could be used to identify individuals, is treated as confidential and stored securely.

Police must balance the benefits of data access with its obligations to hold data securely and protect the confidentiality of information supplied by and concerning individuals. Failing to adequately protect personally identifiable information potentially reduces public trust and confidence in Police, and wider government, which in turn affects the ongoing quality of service associated with data collections.

This document outlines Police's Policy for providing access to its data, resources or privileged information, including relevant legislation and protocols, the principles governing this access, and the requirement for external researchers to enter into a Police Research Agreement. This

Policy applies to all external researchers who request access to Police data, resources or privileged information. It does not apply to journalists or other individuals seeking information pursuant to the Official Information Act 1982.

## **Background information**

### **Definitions**

#### **Data**

Data are non-aggregated or unit record data about the population unit that was sampled. Data include recorded activity associated with any research project and includes interview transcripts, fieldwork notes or other data collected. Data considered here are not necessarily victim statements, interview transcripts or any other recorded activity associated with Police activity.

#### **Datasets**

In this document, sets of data are also referred to as datasets.

#### **Individual information**

Individual information refers to information about a person or organisation.

#### **Privileged Information**

Privileged Information has the same meaning as set out in the Police Research Agreement, and includes any Police information made available pursuant to this Policy and the Research Agreement for research purposes.

#### **Privacy, confidentiality and security**

These terms are often used interchangeably. The following definitions are adapted from Official Statistics System (OSS) Protocols.

1. Privacy refers to the ability of a person to control the availability of information about themselves.
2. Confidentiality refers to the protection of individuals' and organisations' information and ensuring that the information is not made available or disclosed to unauthorised individuals or entities.
3. Security refers to how an organisation stores and controls access to the data it holds.

#### **Inappropriate Disclosure**

Inappropriate disclosure is any data or privileged information that is released outside the parameters of this policy such as the public release (accidental or otherwise) of confidential information about an individual or organisation. Privacy principles, Confidentiality and Security methods are applied to datasets available for research to reduce the risk of inappropriate disclosure.

#### **External researchers**

External researchers include the principal researcher and members of the research team.

1. The principal researcher takes overall responsibility for the process of accessing data, and ensuring that all members of the research team meet terms and conditions for access to data.
2. The research team includes the principal researcher and all co-investigators, including all collaborators, researchers, staff and students who are working on the project with the principal researcher.

External researchers include all researchers who request access to Police data, other than those who are employed by Police. An employee of Police who collaborates to conduct research with an external agency, including undertaking research as a student at a University, or with any person external to the organisation is an External Researcher. The Director of Research and Evaluation, in consultation with a member of Police Executive, may declare any researcher not subject to this policy. This may occur when work is a collaboration directed by Police with another agency, where there is an inter-agency Memorandum of Understanding or other form of relationship that is taken into consideration.

### **Datasets available for research**

Most datasets available for external research purposes have been modified to protect individual information without affecting the overall integrity of the research data. Subject to certain terms and conditions these datasets are available to appropriately vetted and approved external researchers for use outside Police.

### **Metadata**

Metadata is information about a dataset, e.g. the method of data collection, and information about the variables and codes included in the dataset.

## **Relevant legislation, protocols and ethics guidelines**

Official statistics are defined in the Statistics Act 1975 as statistics derived by government departments from:

1. statistical surveys; and
2. administrative and registration records, and other documents from which statistics are, or could be, derived and published.

Several pieces of legislation and other guidelines are relevant to official statistics. Excerpts that are relevant to accessing individual information are discussed here; however, these cannot be relied on without reference to the full documents, which should be consulted as necessary.

### **Statistics Act 1975**

The Statistics Act guides the work of agencies that produce official statistics and sets out obligations on Statistics New Zealand to protect the confidentiality of information provided by persons and businesses. While other agencies providing access to their datasets are not subject to this part of the Act, unless it has been collected jointly with Statistics New Zealand, it provides an example of good practice with regard to security and confidentiality of statistical information.

### **Official Statistics System (OSS) Principles and Protocols**

The OSS Principles and Protocols (Statistics New Zealand, 2007) embody key aspects of the Statistics Act as well as the United Nations Fundamental Principles of Official Statistics. The OSS Principles and Protocols apply to Tier 1 statistics, which include Police data:

1. Nature and extent of crime
2. Family violence research
3. Crime victimisation development
4. Offender criminal apprehensions

Tier 1 statistics are the most important statistics, essential to understand how well New Zealand is performing on key measures. Tier 1 statistics:

1. are essential to critical decision-making
2. are of high public interest

3. meet expectations of impartiality and statistical quality, in accordance with the Principles and Protocols for Producers of Tier 1 Statistics:
4. require long-term data continuity
5. allow international comparability
6. meet international statistical obligations.

### Policing Act 2008

The Policing Act outlines quite specific requirements concerning management of some data relating to its employees, to those arrested or detained and to the form of data required to be held. These specific issues are mostly operational. Specifically, researchers must comply with section 50 the Policing Act. Under this section, it is an offence to have Police property without lawful authority, or reasonable excuse.

Of likely relevance to research are the set of principles that apply to Police's dealings with all its duties. These are:

- a. principled, effective, and efficient policing services are a cornerstone of a free and democratic society under the rule of law.
- b. effective policing relies on a wide measure of public support and confidence.
- c. policing services are provided under a national framework but also have a local community focus.
- d. policing services are provided in a manner that respects human rights.
- e. policing services are provided independently and impartially.
- f. in providing policing services every Police employee is required to act professionally, ethically, and with integrity.

Exercising these principles generates the need to apply considered standards for the use of data as implied by the other legislative, professional and ethical considerations specified in this policy.

### Privacy Act 1993

The Privacy Act is designed to promote and protect individual privacy. It establishes principles with respect to collection, use and disclosure of information relating to individuals. While there are exceptions that permit use for statistical or research purposes, it is good practice to adhere to the principles where possible.

### Official Information Act 1982

The Official Information Act makes official information more freely available, provides for proper access by each person to official information relating to that person, and protects official information to the extent consistent with the public interest and the preservation of personal privacy.

### Code of Professional Standards and Ethics

The Royal Society of New Zealand Code of Professional Standards and Ethics is compulsory for Society members and a voluntary code for all other persons involved in science, technology, and the humanities in New Zealand. It can be found at: <http://www.royalsociety.org.nz/organisation/about/code/>.

### Operational Standard for Ethics Committees

The Operational Standard for Ethics Committees (Ministry of Health, 2006) provides guidance on principles that should be considered when reviewing research proposals, and sets out consistent operational and administrative procedures common to all ethics committees. The

Police Research Agreement requires external researchers to have their research approved by an accredited institutional ethics committee or reviewed by a recognised human ethics body.

### Public Records Act 2005

The Public Records Act is relevant to long-term retention and disposal of records, not to providing access to active datasets.

### The Protective Security Requirements (PSR)

The Protective Security Requirements outlines the NZ Government's expectations for managing personnel, physical and information security. The PSR consists of 29 mandated requirements that are designed to ensure official government information is appropriately managed, handled and available to the right people for the right purpose.

## Principles of Access to Resources, Data or Privileged Information

The Police Policy for External Researchers' Access to Resources, Data or Privileged Information (the Policy) consists of an overall principle, and seven key principles relating to data, purpose, researchers, quality, confidentiality, security and review and modification.

### Overall Principle – Access to data and resources for research

Police will make available the best possible quality data and facilitate access to resources for research:

1. in as much detail as is necessary and possible
2. as widely as practicable
3. as soon as possible
4. as conveniently as is reasonable having regard to the impact on the activities of the Police

while ensuring all legislative and ethical obligations governing access to, and safekeeping of, individual information are followed.

### Principle 1 – Data and Resources

*We will make almost anything available for research.*

- 1.1 Any data of suitable quality that is owned (or managed) by Police is potentially eligible for research use.
- 1.2 The process for making decisions on access to data or access to Police resources will be transparent.
- 1.3 Datasets will be produced in accordance with Principle 4 (Quality) and Principle 5 (Confidentiality).
- 1.4 Access to data and Police resources are subject to the level of demand, availability of resources and confidentiality risk.
- 1.5 Where Police does not have the authority to provide access to data, access is subject to the agreement of the data owner, including any additional terms, conditions and processes specified by the data owner.
- 1.6 No ownership of data is conferred on researchers.

- 1.7 Where data are no longer considered suitable for research use they may be withdrawn from access and will be disposed of (archived or destroyed) in line with the Public Records Act 2005 and in accordance with the NZ Protective Security Requirements as defined by the NZ Information Security Manual instructions for sanitisation, disposal and destruction of media and information..

## Principle 2 – Purpose

*Research must be for public good.*

- 2.1 Research must not be inconsistent with the purposes for which the data were collected.
- 2.2 Research must be for public good purposes, with value and benefits for New Zealand. Access to resources or data is unlikely to be permitted where people or organisations stand to gain commercially.
- 2.3 The value of using Police resources or data rather than other sources of information, or the use of other resources must be shown.
- 2.4 Research must be achievable using the data (i.e., it must be valid and possible), based on scientifically sound methodology, and satisfy any appropriate research ethics requirements.
- 2.5 Research results must be made publicly available. Police must be informed prior to the dissemination of results, such as publications and presentations, in order to be aware, in advance, of potential public interest.
- 2.6 Researchers are expected to commit to undertaking research and disseminating results in a timely manner.

## Principle 3 – Researchers

*We want to engage with researchers and their organisations.*

- 3.1 Researchers proposing research consistent with Principle 2 (Purpose) are eligible to apply for access to Police data and resources, subject to the following criteria:
  - They are connected to a recognised organisation.
  - They have a proven history of public good research or are supervised by a person with a proven history of public good research.
  - Where necessary the research team includes a researcher (statistician/analyst) with recognised skills in analysing data.
  - They meet the requirements of the Protective Security Requirement Personnel Security standards.
  - A student cannot be the principal researcher.
- 3.2 Access to data being offered by this Policy is granted as a privilege not a right. In collecting these types of data Police has an obligation to individuals to protect their information. All researchers must agree to accept these obligations by adhering to terms and conditions of access and relevant legislation and protocols as set out in this Policy and the Research Agreement.

## Principle 4 – Quality

*Researchers are expected to produce good quality outputs that are subject to acceptable quality assurance processes.*

### *Quality of datasets*

- 4.1 Datasets provided to researchers will be of the best possible quality, containing as much detail as possible, notwithstanding data integrity and the need to safeguard individual information.
- 4.2 Datasets will be supported by sufficient metadata to allow appropriate research.

### *Quality of outputs*

- 4.3 Researchers are expected to produce good quality outputs that are subject to acceptable quality assurance processes.
- 4.4 Researchers must follow any quality rules and statistical obligations stipulated in the metadata, by Police and/or by the data owner.

## **Principle 5 – Confidentiality**

### *Confidentiality of individual information will be maintained.*

- 5.1 The confidentiality of individual information will be maintained by modifying datasets to reduce inappropriate disclosure risk without affecting the integrity of the data: All details will be removed that are likely to lead to spontaneous recognition and identity of an individual.
- 5.2 Datasets will be modified so that the identification of individual information is unlikely without a disproportionate amount of time, effort and expertise on behalf of an outside party who has a disclosure to the data.
- 5.3 Researchers must apply the Privacy Act 1993 principles and any confidentiality rules stipulated in the metadata, by Police and/or by the data owner, before outputs are released.
- 5.4 In addition, researchers must ensure that outputs are presented in such a way that individual information is safeguarded should dataset modification and confidentiality rules be insufficient protection.

## **Principle 6 – Security**

### *Researchers will maintain the security of individual information by complying with relevant terms and conditions.*

Despite steps taken to ensure effective confidentiality of data, it is important to also protect the security of datasets in the event that the dataset modification is insufficient and to prevent public concerns or perceptions about how official Police and individual information is being used.

- 6.1 Researchers will maintain the security of official Police and individual information by complying with relevant terms and conditions in the Police Research Agreement with regard to access, use, storage, sanitisation and disposal of information and datasets.

## **Principle 7 – Review, modification and audit**

### *To ensure research meets the intent of this policy and its principles, Police will periodically undertake an independent audit of some external research.*

- 7.1 This Policy and principle will be updated as required to ensure it remains relevant and workable for both Police and researchers.
- 7.2 Police will periodically undertake an audit of some external research projects.



## Requirement to enter into a Research Agreement

1. The organisation responsible for the research team must enter into a Police Research Agreement, which sets out specific terms and conditions with which the researcher(s) must comply. Police may additionally require, before granting research approval and entering into a Research Agreement, that members of the research team undergo Vetting checks. Individual researchers failing the Vetting standard may only be granted access at the discretion of the Director Research and Evaluation in consultation with a member of the Police Executive.
2. The principal researcher and all members of the research team must sign the Police Research Agreement to be granted status as authorised researchers. The principal researcher must send a copy of the signed Police Research Agreement to Police, retain the originals on file and make them available for audit, as required.
3. The research team will be responsible for all research undertaken and ensuring the quality, confidentiality, privacy and security of all information and data associated with the research project. No support will be provided by Police staff unless they are formal collaborators on a project, apart from that necessary to ensure that sufficient information is available to allow the proposed research to be undertaken.

## Dataset production

Police will follow a standard process for creating data, as follows:

1. Ensure the data will have no personally identifiable contact details, such as name and address, or other identifying information likely to lead to spontaneous recognition of a person or an individual record.
2. Undertake a preliminary assessment of inappropriate disclosure risks and the ability to adequately protect data. This includes considering the extent to which it is possible to protect the dataset without disproportionate effort whilst retaining a dataset of value. Potential difficulties in protecting the dataset might arise because of the sensitivity and/or identifiability of the data or because of publicly available data that could compromise the ability to sufficiently protect the dataset.
3. Produce the data and associated risk assessed documentation.
  - a. Aim to standardise data production as much as possible to reduce the time and resources required to create it and to eliminate as far as is possible the risk of different data inadvertently compromising confidentiality protection.
  - b. Produce metadata, including the disclosure control processes (where possible) and potential limitations of the data that are likely to result from the disclosure control process.
  - c. Identify any rules that researchers will be required to apply to ensure the quality and confidentiality of outputs (e.g. minimum cell size, weighted outputs).
4. Costs to produce the data may be recovered from the researcher.



## Comments and feedback

Researchers are welcome to provide comments on their experiences with accessing Police data, resources or privileged information pursuant to this Policy to [research@police.govt.nz](mailto:research@police.govt.nz).

## References

- Lowrance W. 2002. *Learning from Experience: Privacy and the Secondary Use of Data in Health Research*. London: The Nuffield Trust.
- Ministry of Health. 2006. *Operational Standard for Ethics Committees: Updated edition*. Wellington: Ministry of Health.
- National Ethics Advisory Committee. 2006. *Ethical Guidelines for Observational Studies: Observational research, audits and related activities*. Wellington: Ministry of Health.
- Statistics New Zealand. 2007. *Principles and Protocols for Producers of Tier 1 Statistics*. Wellington: Statistics New Zealand.