



MPI Organisational Procedure
*Information Gathering
and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

Information Gathering and Public Trust

DRAFT



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

OVERVIEW

Purpose

MPI has multiple and complex information gathering functions, and we need to ensure that we use our authority to gather information in a way that is lawful and supports public trust. Being vigilant about how we exercise the significant responsibilities and powers entrusted to us by New Zealanders is fundamental to the integrity of the public service, and to our ability to protect and grow New Zealand.

This procedure document supports the MPI Organisational Policy on *Information Gathering and Public Trust*. The policy and procedure documents provide guidance for staff on making good decisions about information collection, to help ensure MPI's information gathering activities are lawful and uphold public trust in MPI.

This procedure document will be reviewed two years from publication (or earlier if significant changes are required).

Background

In December 2018, the State Services Commissioner published [Model Standards on information gathering and public trust](#).

These and other Model Standards on what it means to act in the spirit of public service are published using the Commissioner's powers in section 57(4) of the State Sector Act 1988 to set minimum standards of integrity and conduct for the public service. These particular Model Standards on information gathering (the Model Standards) were published as a result of the [SSC's inquiry into the use of external security consultants](#) (report released 18 December 2018). The inquiry uncovered failings across the public service, including breaches of the State Services code of conduct, and the State Services Commissioner introduced these new standards to strengthen transparency and consistency across all government agencies.

The State Services Commissioner's expectations are that government agencies will be fully compliant with the Model Standards, including publishing a Transparency Statement to explain the ways MPI collects information, including personal information, and why we collect it, and how we use it.



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

SCOPE

All MPI information gathering for regulatory compliance, law enforcement or protective security functions will be carried out in accordance with the MPI Organisational Policy *Information Gathering and Public Trust* and with this Procedure document. This procedure document sets the requirements when developing/reviewing other information gathering policy, procedure and guidance documents.

This procedure document also contains guidance on MPI's approach to:

- verification and validation of information;
- dealing with illegally obtained information;
- working with other government agencies to gather information; and
- the use of external security consultants.

Who this procedure document applies to

This procedure document applies to all staff, contractors and service providers, employed or engaged on any basis by MPI, whether they are casual, temporary or permanent, whether full time or part time and whether they are located in New Zealand or in any other country, and to any delegations being exercised by MPI staff on behalf of other state sector organisations.

This procedure document also applies to all MPI staff using information gathering powers on behalf of other state service organisations, and to MPI's management of industry partners when they are collecting information on MPI's behalf.

Offshore staff should take into account local legislation and regulatory requirements, and seek advice from local advisers where appropriate.

What this procedure document does NOT cover

This policy does not apply to information collected solely for the purpose of delivering functions and services to New Zealanders and businesses. These functions are out-of-scope, and examples include work on the Organism Ranking System, Culex sitiens eradication, TSE surveillance, and myrtle rust programme. Also excluded is the collection of administrative information (including personal information) in the course of conducting MPI's business or delivering services, and information collected to support internal investigations.)

What this procedure document covers

This procedure document covers information collected to give effect to MPI's responsibilities for any of the following:

- to ensure regulatory compliance;
- to detect and deter offending (law enforcement); and
- to protect people, information and places (protective security functions).



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

This policy also applies where information is collected for reasons that include regulatory compliance, law enforcement and/or protective security, as well as to deliver functions and services to New Zealanders and businesses.

All MPI contracts and delegations from other state sector organisations to MPI staff relating to information gathering activities covered by this procedure document must contain obligations that reflect this procedure document.

The information this procedure document applies to

MPI collects information in a variety of ways, using different mechanisms such as statutory powers or by voluntary provisions, or by purchasing it. This procedure document applies to information regardless of how it is obtained, including unsolicited information that is provided to MPI. For example:

- using statutory powers to gather information (for example, production notices and search powers, and the declaration obligations for travellers and goods entering/exiting New Zealand);
- accessing publicly available information (including open source online information);
- purchasing information from external providers;
- information voluntarily provided to MPI (including where a third party makes a decision to release information under Information Privacy Principle 11(e) (of the Privacy Act 1993);
- unsolicited information provided to MPI by third parties (including Protected Disclosures, confidential informants, and activist groups).

“Information” has a similarly broad meaning, including information intended to be used as evidence in litigation, and information that is confidential (for example, intelligence or information shared under restricted conditions).



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

APPLYING MPI'S INFORMATION GATHERING PRINCIPLES

MPI's information gathering principles

The principles are set out in the MPI Organisational Policy *Information Gathering and Public Trust*. They must be taken into account when deciding whether and how to gather information for regulatory compliance, law enforcement and protective security purposes.

The principles are intended to support good decision-making about whether an information gathering activity is legally permissible, as well as whether the activity is appropriate. The guidance below is intended to help you apply the principles.

Principle 1: Our actions are lawful

This principle lists the Acts we need to ensure our actions comply with, in addition to the relevant MPI legislation. This includes:

- Privacy Act 1993, in particular the information privacy principles (section 6).
- Search and Surveillance Act 2012, in particular Parts 3 and 4.
- New Zealand Bill of Rights Act 1990, in particular sections 14-17 and 21.

Principle 2: We have a clear purpose

Demonstrating this principle in action means documenting the rationale for the information gathering activity.

Routine activities occurring regularly or frequently can be documented once for the ongoing activity; any changes (e.g. in scope of the information sought, or the law) mean that document must be reviewed to ensure our activity is lawful and appropriate.

Principle 3: The method is appropriate

Balancing the following factors will help ensure the methods used are proportionate to the rights involved:

- Type of information sought.
- Suspected offending (if any).
- MPI's statutory duties.
- The public interest in regulatory compliance and enforcement or protective security and in avoiding prejudice to the maintenance of the law.
- The extent of intrusion into a person's privacy, property and other rights.
- Whether that intrusion is authorised by specific legislation, and is reasonable in terms of section 21 of the New Zealand Bill of Rights Act 1990.



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

When working out what actions are proportionate, it's important to remember that while the rights affirmed by the New Zealand Bill of Rights Act are subject to reasonable limitation in a free and democratic society, breaches of those rights will be examined both internally by MPI, and scrutinised externally by Ministers, the courts and the media. To maintain public trust in MPI it's important we ensure we use our authority to gather information lawfully and appropriately.

Principle 4: We are transparent and accountable

The MPI Organisational Policy *Information Gathering and Public Trust* for information gathering and public trust requires all information gathering activity for regulatory compliance, law enforcement and protective security to be governed by a documented process.

Where a written procedure does not yet exist, the relevant business unit must notify the owner of this procedure document. The absence of a written procedure does not prevent the particular information gathering activities, but should be rectified promptly.

Principle 5: Acting with integrity, respect and professionalism

All MPI contracts relating to information gathering activities covered by this procedure document must contain obligations that reflect this procedure document.

This includes where MPI employs someone and it is likely they will be engaged in information gathering for regulatory compliance, law enforcement or protective security functions.

See also the section below on information gathering restrictions.

Principle 6: We are trained on how to gather information in accordance with the law and these principles.

Training includes activities to raise or increase awareness and for development of capability.

Role and/or function-specific training should be provided to staff, contractors and service providers on the application of this policy and on how to incorporate it into their procedures for specific information gathering activities. Training should also be provided to support staff working in these areas, to help them understand and navigate the important issues of professional distance and public perception associated with the exercise of their powers.

Training should be both at induction and on an ongoing basis as required.



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

VERIFICATION AND VALIDATION OF INFORMATION

As well as information sought from third parties, MPI sometimes receives unsolicited information that has been gathered by third parties. This information may need to be verified.

MPI staff (including any contractors) will raise concerns promptly where information appears to have been obtained unlawfully or inappropriately (see also the section below on dealing with illegally obtained information). Those concerns will be raised with the manager or Director of the relevant business unit, or advice and guidance can be obtained from: Human Resources; Audit, Risk and Evaluation; Security & Privacy; or Legal Services.

Verification

When information is received, enquiries should be made to determine the veracity of the information where possible. The extent to which you will verify information obtained from third parties will be determined by a range of factors, including:

- The importance of the information being accurate and up-to-date.
- The third party's compliance or other history known to MPI.
- The source of the information:
 - o Information obtained from an anonymous or confidential informant may need to be verified with other sources before further action is taken. The steps taken may depend on the purpose for which MPI intends to use the information, the likelihood of verification causing an adverse impact for the third party, the credibility of the source, and the ease with which information can be verified.
 - o The type of entity the information comes from. For example, information obtained under an Approved Information Sharing Agreement with another government agency, or under delegated powers, will not need to be verified.

Unverifiable information, or information from non-credible sources needs to be weighed carefully as the reliability of the information (accuracy) is doubtful.

When deciding what steps are reasonable to take to verify information, you will need to consider the nature and sensitivity of the information, the reliability of the source, the activity used to gather the information, and the availability of other sources and/or powers to validate the information.

DEALING WITH ILLEGALLY OBTAINED INFORMATION

If you receive unsolicited information that has been obtained illegally, this section explains when it must be referred to the New Zealand Police. You should also take legal advice on your dealings with the information provider because you must maintain professional distance with third parties, and also ensure MPI does not encourage people to obtain information by illegal means or otherwise inconsistently with the [code of conduct for the State Services](#).

Where information needs to be used as evidence in proceedings, refer to the test under section 30 of the Evidence Act. This is because it is the role of the New Zealand courts to make a determination as to whether or not evidence has been obtained improperly (and if so, whether exclusion of that evidence is a proportionate response). This means that it will not necessarily follow that information obtained illegally will never be used by MPI, but that there are several aspects to consider when deciding what to do with the information.



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

If information has been obtained by a criminal act, MPI will not use it as evidence unless there is a realistic prospect the court will admit it under section 30 of the Evidence Act. Sometimes further inquiries will produce other information that mean MPI no longer needs to rely on the potentially improperly obtained information. You should seek legal advice if you are concerned about the original information tainting the collection of this other information.

MPI staff (including any contractors) will raise concerns promptly where information appears to have been obtained unlawfully or inappropriately (see also the section below on dealing with illegally obtained information). Those concerns will be raised with the manager or Director of the relevant business unit to assist with ensuring MPI reports information obtained by criminal acts to the New Zealand Police (unless the Protected Disclosures Act 2000 applies, in which case, follow [MPI's policy for protected disclosures](#)). Advice and guidance can be obtained from: Human Resources, Audit, Risk & Evaluation; Security & Privacy; or Legal Services.

For example, if the information relates to animal welfare offending, the appropriate person to consult with is the Manager Compliance Investigations or the Director Compliance.

WORKING WITH OTHER GOVERNMENT AGENCIES

MPI shares information and works collaboratively with other agencies to increase its effectiveness and efficiency, particularly where there are joint or overlapping areas of responsibility. Information is sometimes shared between MPI and other government agencies, in the course of specific operations or under information sharing arrangements (for example, Memorandum of Understanding, Approved Information Sharing Agreements).

All MPI information sharing for regulatory compliance law enforcement or protective security functions will be carried out under a documented process and with joint governance arrangements in place ahead of delivery: this means ensuring there's a documented explanation of the legal authority for sharing information, and clearly assigned decision-making as well as lead accountability for ensuring the agreed arrangements are effective and align with MPI policies for gathering and sharing information.

We will ensure that before information is shared, we have checked whether the information is subject to legal privilege or other confidentiality, or any statutory restrictions about sharing the information.

USE OF EXTERNAL SECURITY CONSULTANTS

External security consultants are one way in which government agencies can decide to collect information. When contracted by a government agency, external security consultants are acting as an extension of the agency itself. Government agencies may be liable for the actions of third party contractors.

External security consultants cannot be used to undertake information gathering that would not be lawful and ethical for MPI's own staff to undertake.

Before engaging external security consultants to gather information, approval from the business unit's Director must be obtained, along with advice from Legal Services as to whether the use of the external security consultant is appropriate in the particular circumstances.



MPI Organisational Procedure
Information Gathering
and Public Trust

Owner: Director,
Business Tech & Info
Services

Published: select date

When deciding whether or not to use external security consultants, you must consider:

- the need for a robust contract, ensuring compliance with this procedure document, the MPI Code of Conduct, the State Services Code of Conduct, the Public Records Act 2005, the Official Information Act 1982, and the Privacy Act 1993;
- awareness of MPI staff of the issues to be careful of when working with external security consultants;
- whether the provider is on the All-of-Government panel for external security consultants;
- the importance of a robust procurement process, including that suppliers and any subcontractors:
 - have the necessary licences;
 - are compliant with the Private Security Personnel and Private Investigators (Code of Conduct - Surveillance of Individuals) Regulation 2011; and
 - understand their obligation to declare conflict of interest, and that MPI works with them to managed these appropriately.

DRAFT



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

REQUIREMENTS FOR INFORMATION GATHERING POLICIES, PROCEDURES AND GUIDELINES

All MPI information gathering for regulatory compliance, law enforcement or protective security functions will be:

- carried out in accordance with this procedure document and with the principles in the MPI Organisational Policy *Information Gathering and Public Trust*; and
- supported by a written procedure and training.

When developing new policies and procedures, or updating existing ones, this procedure document must be integrated into information gathering policies and processes associated with MPI's regulatory compliance, law enforcement and security functions.

MPI business unit undertaking the information gathering activity will review their information gathering procedures at regular intervals, or when there are significant changes to the regulatory environment (for example, a decision of a tribunal or court concerning information gathering).

New activities/changes to activities

The MPI information gathering principles must be incorporated into decisions relating to new information gathering activities. This includes decisions about new methods of information gathering and new operations utilising existing methods. These decisions will be informed by a privacy impact assessment if personal information is being gathered.

Where a decision affects only one business unit or branch, approval is required from an appropriate manager or Director, except in cases where the decision-maker has an independent statutory role or there are legislative or security restrictions.

Undertaking new information gathering activities for regulatory compliance, law enforcement or protective security purposes must be approved by the Director(s) responsible for the staff undertaking the activity, and should be notified to the Director responsible for the MPI Organisational Policy *Information Gathering and Public Trust*.

Content of information gathering policies/procedures/guidelines

Information gathering policies and procedures will include:

- an explanation of the specific information gathering activity, the legal authority for it (legislation, case law) and the MPI purpose (function) it relates it;
- the scope of activity, including information sources, an explanation of why and how information is to be collected, analysed, stored, and what steps (if any) should be taken to verify and validate information sources);
- the decision-making framework and process that staff should follow when considering such activity (including when a warrant should be sought);
- the training provided to staff;
- whether legal advice must be sought;
- any specific complaint or review mechanism available (and where none exist, a reference to the mechanisms described in this procedure document);



MPI Organisational Procedure
*Information Gathering
and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

- guidance on the use, sharing, storage and destruction of any information collected;
- a privacy impact assessment where personal information is being collected;
- a health and safety risk assessment specific to the activity/activities (including a plan for responding to threats if an activity-specific plan is needed); and
- a review timetable for the policy/procedure.

DRAFT



MPI Organisational Procedure *Information Gathering and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

OVERSIGHT

MPI has several mechanisms providing governance, assurance, investigative and/or operational oversight across MPI, that will also have a role in providing oversight of information gathering activity. Oversight includes reviewing governance, accountabilities, policies and processes, and recommending improvements to them to ensure MPI is compliant with the MPI Organisational Policy *Information Gathering and Public Trust*, this procedure document and the [Model Standards for information gathering and public trust](#).

The efficacy of this approach will be reviewed by 30 June 2020.

Refer to the Key Accountabilities section of the Organisational Policy *Information Gathering and Public Trust* for more information.

BREACHES OF THIS PROCEDURE DOCUMENT

A breach of this procedure document or the Model Standards does not necessarily render MPI's actions unlawful or mean evidence will not be admissible. Non-compliance with this procedure document or with the Model Standards on information gathering and public trust does have several consequences, including potential reputational harm for MPI, financial loss (including damages claims), challenges to the admissibility of evidence in proceedings, and consequences for breach of employment and contract obligations.

Non-compliance relating to MPI employees or contractors will be managed in accordance with processes for breach of the [MPI Code of Conduct](#).

Where breaches of the procedure document have the potential to impact the admissibility of information as evidence, you will need to consider the test in section 30 of the Evidence Act 2006.

Seek advice from your manager or Director, or from Human Resources, Security & Privacy or Legal Services if you have concerns. The MPI Organisational Policy *Information Gathering and Public Trust* also contains contact information for assistance and advice.



MPI Organisational Procedure
*Information Gathering
and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

OTHER REFERENCES

MPI is responsible for administering a large variety of legislation, a number of which require and authorise information gathering in order for MPI to meet its statutory obligations.

The following legislation is related to this procedure document:

- Privacy Act 1993, in particular the information privacy principles (section 6).
- Search and Surveillance Act 2012, in particular Parts 3 and 4.
- New Zealand Bill of Rights Act 1990, in particular sections 14-17 and 21.
- Health & Safety at Work Act 2015.
- Crimes Act 1961.

This is not an exhaustive list and other legislation or regulations will apply to particular MPI business units' information gathering activities. Legislation that MPI administers or exercises delegations under may contain specific provisions and powers relating to information gathering, for example:

- Animal Welfare Act 1999
- Biosecurity Act 1993
- Fisheries Act 1996
- Food Act 2014
- Climate Change Response Act 2002

Guidance material

The policy owner is authorised to issue guidelines to support this policy.

DRAFT



MPI Organisational Procedure
*Information Gathering
and Public Trust*

Owner: Director,
Business Tech & Info
Services

Published: select date

Document Information

Date	Version	Author	Comments
21/05/2019	1	Kahla Parkash, Principal Legal Adviser	Initial draft
13/06/2019	2.0	Kahla Parkash, Principal Legal Adviser	Version for consultation with MPI Organisational Policy Committee.
25/06/2019	3.0	Kahla Parkash, Principal Legal Adviser	Incorporates feedback from consultation.
26/06/2019	3.7	Kahla Parkash, Principal Legal Adviser	Version for sending to Director-General/06
27/06/2019	3.8	Kahla Parkash, Principal Adviser	Updating business unit names where confirmed; incorporating changes from Learning & Development.

DRAFT