MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

IMMIGRATION

IN CONFIDENCE

Immigration New Zealand

Information Gathering Procedures

V1.0 –30 April 2019

New Zealand Government

Contents

Document Control

Document Owner(s)

Name	Title / Position
Stephen Dunstan	General Manager, Service Design and Performance

Ownership of Procedure

Title / Position
General Managers

Version Control

Version	Date	Author(s) Name/Position	Specific Areas Updated
0.1		Elizabeth Cantrick	First draft
0.2 – 0.3	12 April 2019	Meegan Sorenson/ Sarah Kemp	Working drafts
0.4	24/26 April 2019	Elizabeth Cantrick/Sarah Kemp	For ILT endorsement
FINAL v1.0	29 April 2019	Elizabeth Cantrick	FINAL

Introduction

Purpose

The purpose of this document is to provide guidance to INZ staff on information gathering procedures when exercising the responsibilities and powers granted to them for the collection, storage and use of all information gathered to ensure regulatory compliance with the Immigration Act 2009 and other related legislation.

Background

Information gathering by government agencies is governed by a legislative framework that includes the requirements of agencies' own legislation, and their responsibilities under the Privacy Act 1993.

When agencies gather information for regulatory compliance and law enforcement purposes they are exercising the powers of the State. Parliament has given them authority to ensure that the law and due process is being followed. It is important that agencies act in accordance with this authority and in line with what the public generally expects and considers reasonable. This is fundamental to fostering New Zealanders' trust and confidence in the public service.[1]

It is important that INZ gathers; stores and uses information in accordance with its delegated authorities and responsibilities.

Who do these guidelines apply to?

These procedures apply to all staff, contractors and service providers, employed or engaged on any basis by MBIE, 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.

These procedures apply to:

- information that MBIE gathers for its law enforcement, regulatory compliance, and protective security functions; and
- information gathering activities to take any action or decision regarding penalties, sanctions, offences or prosecution under any legislation or regulation that MBIE administers or is responsible for. This includes taking action where a regulated party does not do something (e.g. does not comply with a permit, license, condition or visa).

While the primary focus of these guidelines relate to information gathering for law enforcement, regulatory compliance, and protective security functions, the general principles outlined in this document are equally applicable to business-as-usual service delivery functions for example visa decision making, business support or attraction and marketing activity.

These procedures should be read in conjunction with MBIE's Information Gathering Policy http://thelink/tools/policies/Pages/Informationgathering.aspx and where applicable individual next-level business unit procedures.

- CRIS
- Visa Services
- SPA
- SDP

MBIE's information gathering principles

These principles must be taken into account when considering, or undertaking, information gathering activities. The principles are intended to assist with deciding both whether an

[1] SSC Model Standards Information Gathering and Public Trust

information gathering activity is legally permissible (i.e. **can** the information be gathered), and whether the activity is appropriate for MBIE to undertake (i.e. **should** the information be gathered).

Considered Is the most appropriate authority or legislative tool being used to gather the information? Even if it is legally possible, is the information gathering reasonable?	**Necessary** Gather only information that is necessary for the MBIE function
Proportionate Only collect the minimum amount of information proportionate to the purpose of the proposed activity	**Transparent** Would the general public, or other stakeholders, be surprised by the information gathering activity? The information gathering is documented
Accountable All information gathering is governed by a policy and is supported by a procedure Gathering policies and procedures are reviewed and approved by a person or group not directly involved in the gathering or the function the gathering relates to	**Integrity** Keep professional distance Act impartially, in accordance with legislative mandate Take into account additional obligations on public sector agencies who have regulatory powers – SSC and MBIE Codes of Conduct
Respectful Take into account: i. Impact on vulnerable community members (including children) ii. The operation of the Search and Surveillance Act, and relevant considerations including te ao Māori principles iii. Any privileged information held by an individual iv. Privacy v. Other protections in the Bill of Rights Act, including the right to freedom of expression	

Definitions

Word	Meaning
MBIE	Ministry of Business Innovation and Employment
INZ	Immigration New Zealand
Information	Both personal and non-personal information, and includes any information, fact, opinion or intelligence that does or could assist MBIE to fulfil or improve its regulatory compliance, law enforcement, or protective security functions – either alone or with another agency. Information may include: written information (notes, reports); visual information (photographs, videos); technical information (GPS location data)
Gathering activity	Includes obtaining information from the following sources: The Internet (websites, Google searches, social media including Facebook Phone calls Interviews (voluntary and compulsory)

	searches)		
	Tip-offs	Written requests/emails	Databases
	Information feeds (APP information)	Direct system access (AMS, TIKA)	MIU products
	Analytics, trend information	MoUs	Biometric collection
	Public registers and archives	Private records and archives (e.g. employer records)	Technical and scientific devices (GPS devices)
	Production powers (e.g. statutory notices, certificates)	Inspections of places, goods (e.g. site visits)	Requests to other agencies (including NZ govt agencies; private sector agencies, overseas governments and agencies)
PIA	Privacy Impact Assessment		

Information gathering legislation

INZ staff must have a demonstrated understanding of the following legislation when applicable to their role:

Legislation	Application
Immigration Act 2009	Provides authorisation for enforcement and investigative activities.
Immigration Regulations	Provides authorisation for regulatory activities.
Privacy Act 1993	Provides principles for how INZ collects, uses, discloses, stores and give access to 'personal information'.
Bill of Rights Act 1990	Compels INZ to respect individuals' rights to personal privacy, freedom of expression, freedom of peaceful assembly and freedom from unreasonable search and seizure.
Search and Surveillance Act 2012	Facilitates the monitoring of compliance within the law and the investigation and prosecution of offences in a manner that is consistent with human rights values.
Official Information Act 1982	Provides proper access by each person to official information held by INZ relating to that person.
Crimes Act 1961	Forms a leading part of the criminal law in NZ. The Act partially codifies the criminal law in NZ. Most crimes in NZ are created by the Crimes Act, but some are created under common law.

Advice on the interpretation or application of the above legislation can be sought from various sources such as:

- Your Technical Specialist;
- Your Manager;
- Operational Support Team;
- The Ministry's Legal Branch.

Information gathering training

In addition to this Information Gathering Procedures, other training for INZ staff on Information Gathering includes:

- Guide to Privacy
- Security 101
- Doing the right thing at MBIE
- Records Management 101
- Advanced Social Media Training
- Health Safety and Security Induction
- Investigative Interviewing and P.E.A.C.E
- Managing Critical Health, Safety and Security Risks
- Staff Safety and Wellbeing
- Social Media for Verification and Investigation
- New Zealand Certificate in Regulatory Compliance modules one to five (G-Reg)

Use of powers to gather information

Immigration staff are enabled by legislation and a range of legal instruments (e.g. Memorandums of Understanding (MOU's), Approved Information Sharing Agreements (AISA)) to exercise powers that will enable them to gather, share and disclose information. How these operate will vary between business units and roles.

Staff need to ensure that they are aware of and compliant with the information gathering powers applicable to their role. These are explained in more detail in individual business unit next-level procedures.

- CRIS
- Visa Services
- SPA
- SDP

Disclosure of information gathered for immigration purposes

The Privacy Act 1993 states that an agency that holds personal information that was obtained in connection with one purpose (i.e. visa decision making), shall not use the information for any other purpose.

Despite the above, other provisions allow for certain circumstances where personal information can be used for other purposes for example:

- where the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or
- that the use of the information for that other purpose is authorised by the individual concerned e.g. a privacy authorisation is provided.
- Other exceptions include avoiding prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or for the enforcement of a law imposing a pecuniary penalty.

Other relevant legislation includes:

- Pursuant to the Official Information Act 1982 or in accordance with statutory powers to compel information e.g. s 16 of the Tax Administration Act
- Pursuant to sections 294 to 306 of the Immigration Act

Any existing MOU's used for disclosure purposes should comply with at least one of the provisions set out above.

INZ staff must ensure that they are authorised by one of the above provisions to use personal information collected for Immigration purposes for another purpose i.e. providing it to another agency (including another part of MBIE).

When is a Privacy Impact Assessment required?

If teams are considering new ways of collecting, storing, using or sharing personal information, a privacy impact assessment (PIA) should be completed.

MBIE's Privacy Impact Assessment (PIA) Framework describes how to assess an initiative to determine if personal information will be impacted, and if so, provides guidance about how to manage the associated risks.

Information gathering from Social Media

The use of social media for verification and investigation purposes in support of regulatory, compliance and enforcement work needs to be a considered decision. Information gathered from social media may or may not be valuable and, irrespectively, accessing the information carries risks that must be managed.

At a high level, the risks of using social media to gather information for verification and investigation purposes to support regulatory, compliance and enforcement work may be to:

- the rights of New Zealand's citizens and visitors
- the personal safety of staff or their family
- the security of MBIE's ICT network
- MBIE's reputation and legal liability
- the work of other agencies – domestically and internationally – should MBIE's activities inadvertently overlap with their activities.

For this reason, staff wishing to engage in gathering information from social media must gain the necessary approval before doing so and undertake the mandatory training.

For further advice on gathering information from social media refer to the Ministry Procedures for MBIE staff using Social Media policy and/or discuss with your:

- Technical specialist;
- Manager; or
- Operational support team;

Information gathering from the Internet

The following guidelines should be considered when gathering information from the internet:

1. Test the credibility of the data source	- Who is the author? - What qualifications or expertise do they have? - Does the author have contact details? - Is the website objective, unbiased, balanced?
2. Determine data	- How frequently is the site updated? - Is it well maintained and links working?

currency and accuracy	- Is "What's New" actually new? - Is there an editor or editorial board with publishing guidelines?
3. For Open (unregistered) Searching	Staff must follow the **Information Gathering Decision Tree** (Appendix 1).

Verification and weighing of Information

Staff must ensure that any information that they receive or gather for the purposes of exercising powers or other regulatory activity under the Immigration Act 2009 is verified to determine it is accurate and up to date.

Receiving and gathering information from a third party

Information may be received from or gathered from a third party. Examples include:

1. A request to or from another agency
2. Unsolicited information 'dob-in' or 'tip-off'.
3. A person authorised by the individual concerned

Staff must ensure that the information gathering sources for received information are lawful and appropriate i.e. reliable, credible, and appropriate for public sector agencies.

To support his assessment all information received from or gathered from a third party should be verified by the Information Gathering Decision Tree (Appendix 1).

What to do if information has been gathered unlawfully

If it is believed that information may have been unlawfully obtained, unfairly obtained, obtained in an unreasonable or intrusive manner (either internally by INZ or externally by another agency, business entity or a private individual), or has been provided to INZ in error then in the first instance you should advise your immediate manager and obtain advice from MBIE Legal. Also refer to the Information Gathering Decision Tree (Appendix 1).

Information gathering to support joint-agency operations

The MBIE Practice Guidelines: Principles and Procedures for working with Internal/ External agencies in joint regulatory operations provides support to teams involved in joint-agency operations.

Staff involved in the planning of joint-agency operations must ensure that Operation Plans include the appropriate provisions for the sharing of information during all phases of a joint-agency operation.

The following information and templates are also available:

- Joint Assessment Group (JAG) information sharing protocols
- Form for provision of investigative information
- Form for receipt of investigative information

Use of the above forms when gathering or receiving information from other agencies will help provide assurance that the information gathered by other agencies has been gathered appropriately (i.e. not just whether it was gathered lawfully).

Teams involved in joint-agency operations must also comply with MBIE's monthly reporting requirements which centrally record the number of operations undertaken across the Ministry.

Information storage, retention and disposal

INZ has an obligation to manage its records effectively and efficiently, and comply with legislation and codes protecting public records, privacy and evidence. MBIE's Records management intranet page and Records Management Policy provides a framework for assigning record keeping accountabilities and responsibilities to ensure full and accurate records of MBIE's business activities are created.

MBIE's Records Management Policy also sets out the requirements for managing MBIE's records and the information they contain throughout their lifecycle. It outlines staff responsibilities and accountabilities to access, create, maintain and lawfully dispose of records.

All information gathered for immigration purposes should be stored on core immigration systems for example INZ's:

- Application Management System (AMS)
- Case management system - TIKA
- Document management system – MAKO
- Shared office local drives where MAKO or TIKA does not exist.

The following principles apply with respect to Information storage, retention and disposal:

Principle 1 – Create and maintain full and accurate records
Principle 2 - Capture all records into recordkeeping systems
Principle 3 - Make complete, authoritative and reliable records of business
Principle 4 - Ensure records are accessible, usable, retrievable, and preserved
Principle 5 - Records are secure, protected and stored appropriately
Principle 6 - Retention and disposal of records is authorised
Principle 7 - Staff are trained in recordkeeping

Further information on MBIE and INZ's retention and disposal schedule can be found via the following links:

- Visa Services VisaPak advice
- MBIE Records Retention and Disposal Schedule including detailed INZ schedule.

What to do with information that is no longer accurate

Principle 6 and 7 of the Privacy Act 1993 and Part 4 of the Official Information Act 1982 provide guidance on the correction of personal information where an individual makes a request for the correction of that information.

Sections A7.10, A7.70 and A8.65 of Immigration Instructions also provide guidance on the correction of personal information.

Examples include:

- When an individual requests a copy of their file under the Privacy Act 1993 and they disagree with information recorded by INZ
- When an individual advises that they have changed their name or that their date of birth is not accurate or has changed due to being recorded as inaccurate at their birth registration
- When a privacy breach occurs.

Any questions relating to the process to correct information can be directed to:

- Visa Services - the Visa Services Privacy team
- CRIS – CRIS Business Support Team
- SPA

All privacy breaches should be escalated to a manager as soon as possible and reported using the Event reporting tool on your desktop as soon as possible (within 24 hours). This should be done by your manager.

Guidance on minimal personal information

Staff must take particular care in relation to information gathering associated with regulatory compliance, law enforcement and security functions to ensure that information gathering (including the amount and type of information and the way it is collected) is proportionate and reasonable. Essentially, staff in an information gathering role should only gather the minimum amount of information needed to make a decision.

Search and Surveillance Act 2012

In general, Compliance, Risk and Intelligence (CRIS) are the only business unit within INZ that have powers associated with the Search and Surveillance Act 2012. Section D4.14 Search of detained person outlines where those powers are used.

The purpose of the Search and Surveillance Act 2012 is to facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values by—

(a) modernising the law of search, seizure, and surveillance to take into account advances in technologies and to regulate the use of those technologies; and

(b) providing rules that recognise the importance of the rights and entitlements affirmed in other enactments, including the New Zealand Bill of Rights Act 1990, the Privacy Act 1993, and the Evidence Act 2006; and

(c) ensuring investigative tools are effective and adequate for law enforcement needs.

Field work / off site visits

Field work or offsite visits require planning and completion of risk assessments. In some instances planning may require familiarisation with an address and travel route to support Health & Safety planning.

This type of activity is permissible however, wherever possible, open source tools such as Google Maps, Street View should be used to support this planning above driving by premises or locations to ascertain the travel route and any other Health & Safety matters.

If necessary, staff may take a photograph of non-private premises and/or other environmental aspects associated with the visit and/or regulatory powers on an MBIE device. Where this activity is necessary staff should take particular note of the definitions of private activity, private premises, non-private premises and visual surveillance devices as described in section 45 and 46 of the Search and Surveillance Act 2012.

The Bill of Rights Act

All staff involved in information gathering activities will take into account any individual or group protections set out in the Bill of Rights Act 1990.

Staff (including any contractors or service providers) will not gather information on, or classify as a security threat, an individual or group solely on the basis that they are exercising any of their democratic or civil rights, including their legal right to freedom of expression, association, and peaceful assembly to advocate, protest or dissent.

For the avoidance of doubt staff will not gather information:

- about an individual solely based on them being a part of an ‘issue-motivated’ group
- about a group solely because they are an ‘issue-motivated’ group
- about an individual or group solely to manage a risk to INZ or MBIE’s reputation.

Review and assurance

The MBIE Policy for Information Gathering for Regulatory Compliance, Law Enforcement and Protective Security Functions (the MBIE Policy) will be reviewed annually to ensure that it remains fit for purpose.

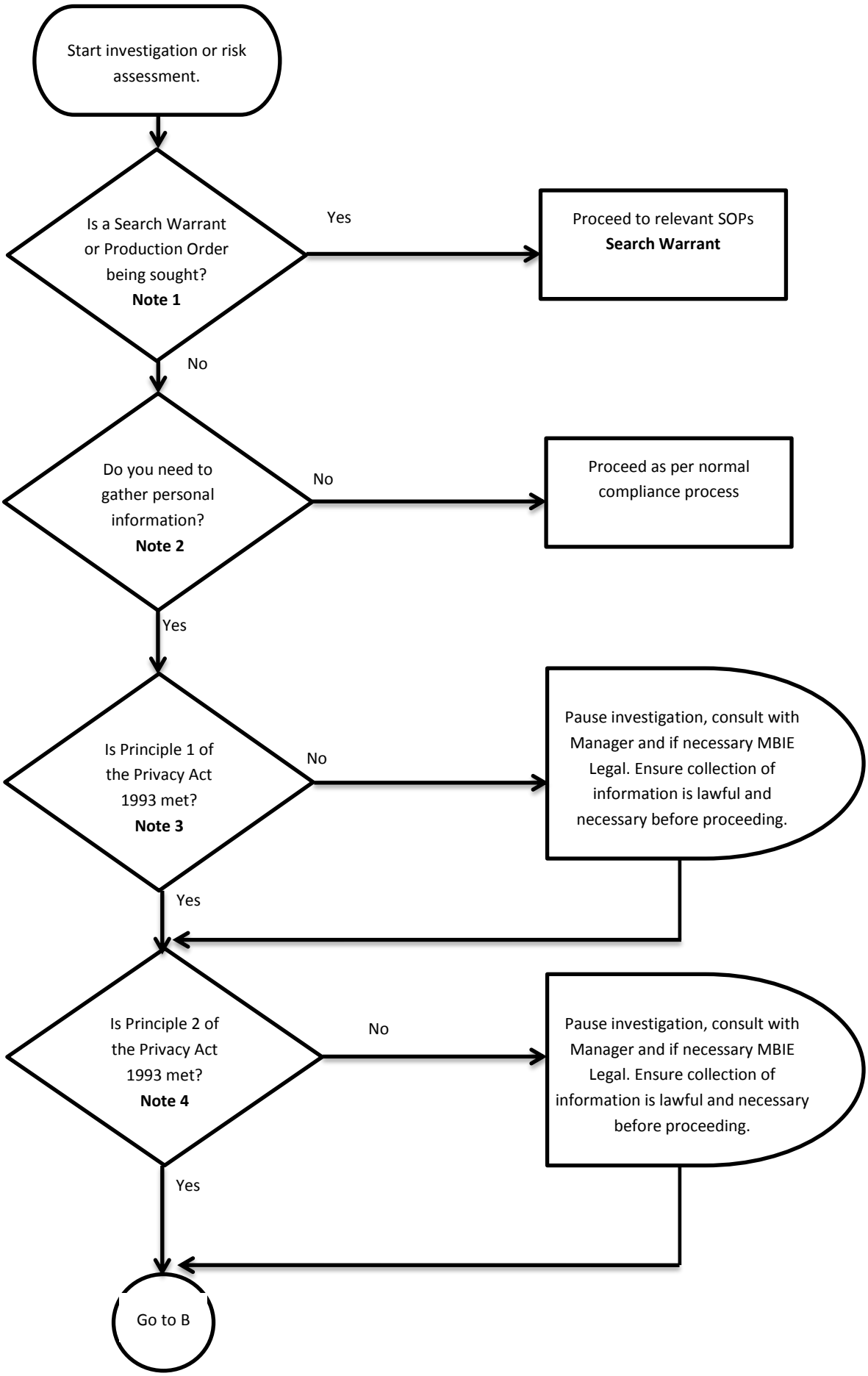
The review of the MBIE Policy will take into account legal, technological and environmental changes, including changes in legislation, governmental priorities, the public's expectations of public sector agencies, and the wider regulatory landscape in which MBIE operates.

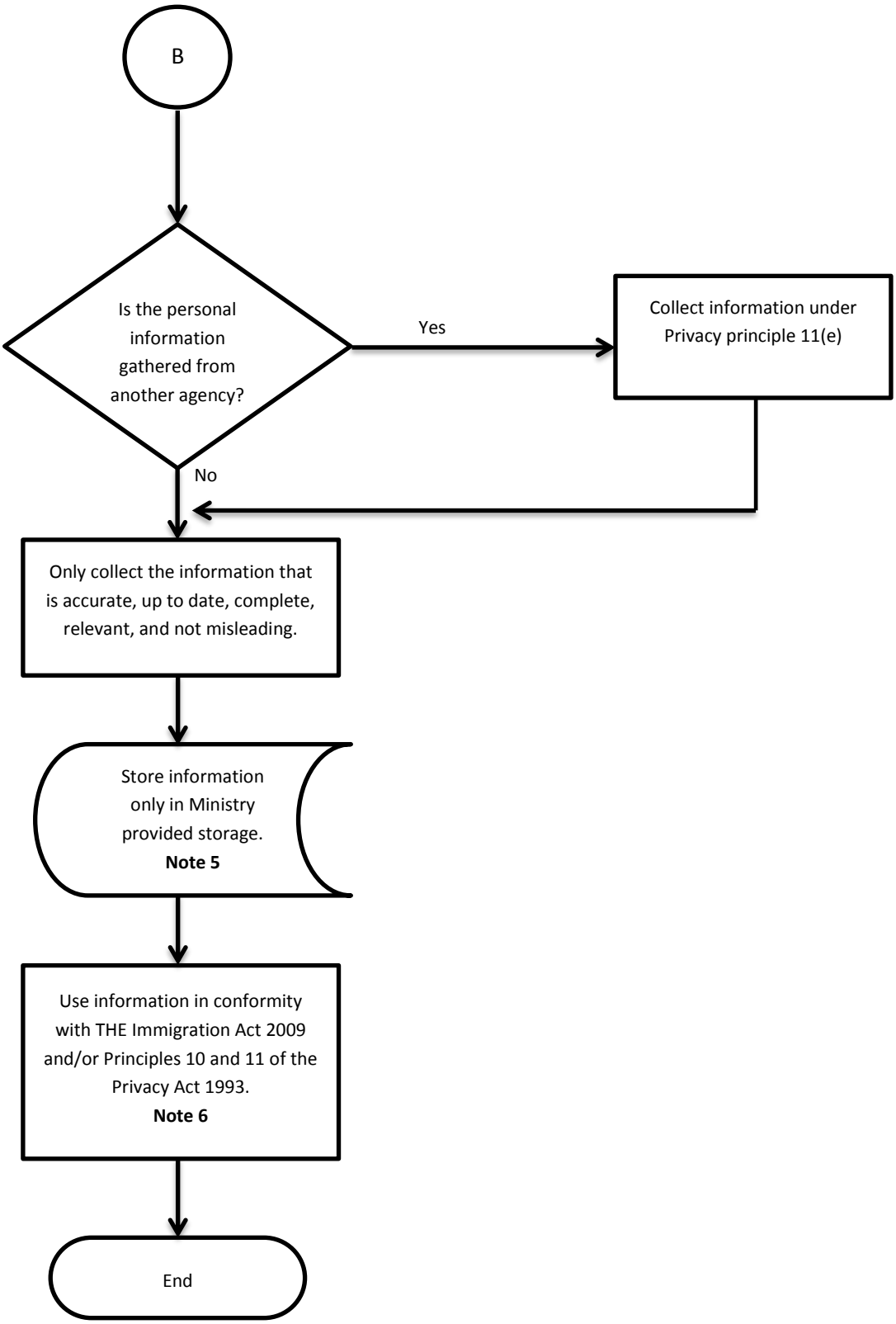
The INZ Information Gathering Procedures will be reviewed annually to ensure they remain fit for purpose. The review of the Procedures will take into account any changes as set out above.

Key Accountabilities and responsibilities

Role	Responsibility
DCE	• Overarching accountability for all INZ information gathering activity and decisions • Approval of these procedures • Embedding of the policy and associated procedures into INZ
GM - SDP	• Business owner of INZ Information Gathering Procedures • Ensuring this Policy remains fit for purpose and in line with MBIE's guidelines on internal management policies • Ensure overarching procedures are reviewed annually • Monitor business unit compliance with information gathering assurance processes
General Managers	• Embedding of the policy and associated procedures into their teams • Business owner of individual business unit next-level procedures • Ensure next-level procedures are reviewed annually • Ensure information gathering assurance processes are undertaken as prescribed in business units assurance programmes
AGM/ 4th tier managers	• Ensure staff are aware of MBIE policy relating to information gathering • Ensure staff are aware of INZ Information Gathering Procedures and business unit next-level procedures • Ensure staff are adequately trained in information gathering best practices • Ensure business unit next-level procedures are reviewed in accordance with business unit assurance programme
All INZ Staff, contractors, suppliers and service providers	• Conduct information gathering activities in accordance with their legislative mandate, this Policy and team procedures • Consider discretionary activities in accordance with the principles in this policy • Promptly raise concerns regarding any information gathering activity that appears unlawful.

Appendix 1 - Information Gathering Decision Tree




B
Is the personal information gathered from another agency?
Yes
Collect information under Privacy principle 11(e)
No
Only collect the information that is accurate, up to date, complete, relevant, and not misleading.
Store information only in Ministry provided storage.
Note 5
Use information in conformity with THE Immigration Act 2009 and/or Principles 10 and 11 of the Privacy Act 1993.
Note 6
End

Notes - Information Gathering Decision Tree

Note 1.

A Production Order is a court granted authorisation to obtain data from a third party (e.g. text messages from a telecommunications company).

Note 2.

Personal information is any piece of information that relates to a living, identifiable human being.

Note 3.

Personal information shall not be collected unless -

(a) The information is collected for a lawful purpose connected with a function or activity of INZ , and
(b) The collection of the information is necessary for that purpose.

Note 4.

(1) INZ shall collect personal information directly from the individual concerned.

(2) It is not necessary to comply with sub clause (1) above if it is believed, on reasonable grounds,-

(a) that the information is publicly available information; or

(b) that the individual concerned authorises collection of the information from someone else; or

(c) that non-compliance would not prejudice the interests of the individual concerned; or

(d) that non-compliance is necessary -

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) that compliance would prejudice the purposes of the collection; or

(f) that compliance is not reasonably practicable in the circumstances of the particular case; or

(g) that the information -

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) that the collection of the information is in accordance with an authority granted under section 54 of the Privacy Act 1993.

Note 5.

Information storage complies with the Ministry Record Management Policy and storage facilities including:

- INZ case management systems e.g. TIKA, AMS and Case Tracker.
- Ministry electronic document and records management system (MAKO).
- Ministry Wide Area Network (WAN) including secured drives and devices.
- Secure store rooms.

The information must be readily retrievable so individuals concerned shall be able to:

(a) obtain confirmation of whether or not INZ holds such personal information.

(b) access that information.

(c) request the correction of that information.

Note 6.

Use of personal information is limited to the purpose for which it was gathered unless use of the information meets the exception conditions of Principle 10 of the Privacy Act 1993.

Disclosure of INZ collected personal information to other agencies can only occur if the other agency makes a request under Privacy principle 11 of the Privacy Act 1993 or if the agency has powers to compel the information from INZ.