



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI

UNCLASSIFIED



Privacy Policy

November 2018
Version 2.3

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Revision history

Version	Date	Author	Description of changes
1.0			Creation
2.0			Annual review
2.1	August 2017	Viv Ching	Contact details amendment
2.2	October 2018	Lee Patton	Review and updates to: <ul style="list-style-type: none"> • Template • Definitions • Accountabilities and responsibilities
2.3	November 2018	Kristina Nelson	Definition MBIE People (Post P&P Committee)

RELEASED UNDER THE OFFICIAL INFORMATION ACT

MBIE Guiding Principles Relevant to This Policy

The Privacy Policy aligns with the MBIE guiding principles of: ensuring a healthy, safe and secure environment; being a good employer; acting with or complying with the law and legislation; and protecting organisational reputation.

Purpose

The Ministry of Business, Innovation and Employment (MBIE) must maintain the trust and confidence of individuals who provide it with their personal information. The purpose of this policy is to ensure that appropriate policies, processes and systems are in place to manage personal information, in line with government, public, and individual expectations, and protect the privacy of individuals.

The legitimate and safe use of the personal information it holds will enable MBIE to improve productivity and business performance, in order to *Grow New Zealand for All*.

Scope

This policy applies to all:

- MBIE people – including permanent staff, temporary staff, and contractors
- third-party service providers who support MBIE to deliver services to staff, customers, clients, and stakeholders
- the personal information that MBIE collects, uses, accesses, shares, stores and disposes of.

Help

Advice and guidance on privacy at MBIE, and managing personal information, is available from the Privacy Team. Contact: privacyteam@mbie.govt.nz

Policy statements

1. MBIE will demonstrate the appropriate standards of care required to ensure that individuals trust it with their personal information.
2. MBIE will be transparent about how it collects, uses, accesses, shares, stores and disposes of the personal information in its care. It will use informed consent wherever possible, to realise the benefits from information while protecting the privacy of individuals.
3. MBIE will maximise the value of the personal information it holds to deliver better public services and improved outcomes for New Zealanders.
4. MBIE will make the personal information it holds available externally to the maximum extent permissible to deliver better public services and improved economic outcomes for New Zealanders.
5. MBIE will promote innovation by combining personal information from internal and external sources, using and sharing this as appropriate, to increase its services' efficiency and effectiveness.

6. MBIE will foster a culture of continuous improvement by having a consistent approach for managing privacy-related business performance and events, and by sharing experiences, failures, successes and best practices.

Definition of terms

Data & Information Steward: the recognised individual who is accountable for a data or information asset on behalf of MBIE. The steward ensures the data or information asset is trusted and reliable and remains fit for purpose as organisational needs and outcomes change over time. Data stewards are responsible for ensuring policy and legislative requirements are met. A steward will often delegate the operational responsibility for information assets to a custodian.

MBIE people: all staff, secondees and contractors, employed or engaged on any basis by the Ministry, 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 who have access to any personal information MBIE holds.

Privacy event: where MBIE (including our contractors and third party service providers) fails to manage personal information in accordance with MBIE's privacy processes and standards. Includes all privacy breaches (where personal information is wrongly collected, used, accessed, disclosed, kept or withheld) and potential privacy breaches ('near misses') (where an action could have resulted in a breach, but the breach does not occur).

Personal information: any information about an identifiable individual.

Key accountabilities and responsibilities

The operating concept for managing privacy at MBIE (including formal compliance and management practices) is based on business unit responsibility for information collection, use and access, information storage and subsequent management (including disposal). This reflects the diversity of business activities and customer groups across MBIE. This delegated model is, however, to be managed within a MBIE-wide framework of information management (including using information effectively to achieve MBIE's full range of organisational objectives), security, reporting and response, and consistent communication with customers.

Role	Description of responsibility
Chief Executive	Accountable for the Privacy Policy.
SLT as the Wellbeing, Health, Safety, and Security Governance Committee	Provides strategic direction and leadership to ensure MBIE is a safe and secure environment for our people, customers and information.
Policy and Procedures Sub-Committee	Considers and endorses MBIE's Privacy Policy in accordance with Internal Policy requirements.
DCE, CGI	Provides leadership on the SLT for privacy and oversight of the delivery of the privacy programme.

UNCLASSIFIED

DCEs	<p>Ensure enterprise privacy risk is assessed within their Groups and for each Branch in their responsibility.</p> <p>Ensure Data Stewards and Custodians meet their responsibilities.</p>
Managers	<p>Use personal information legitimately and safely to deliver MBIE's services effectively and efficiently.</p> <p>Promote innovation by combining personal information from internal and external sources, using and sharing this as appropriate to improve the quality and performance of MBIE's services.</p> <p>Reinforce MBIE's commitment to use and share personal information.</p> <p>Ensure MBIE people are appropriately trained on how to handle personal information, including raising issues and reporting events.</p> <p>Ensure all legal requirements and Ministry-wide policies are complied with when personal information is used and shared within MBIE or other organisations.</p>
All MBIE people	<p>Ensure personal information is managed in accordance with MBIE policies, processes and systems, and practices.</p> <p>Maintain the integrity, accuracy and confidentiality of personal information they deal with.</p> <p>Respond to requests for access and correction made by individuals.</p> <p>Identify privacy events and report these to their manager.</p>
Chief Legal Advisor	<p>The Chief Legal Advisor is MBIE's Chief Privacy Officer.</p> <p>Responsible for MBIE's relationships with the Government Chief Privacy Officer and the Privacy Commissioner.</p> <p>Accountable for the delivery of the Privacy Programme.</p> <p>Ensure appropriate and thorough incident management in the event of a significant privacy breach.</p>
Privacy Steering Group	<p>Provides oversight, guidance, support and direction to the privacy programme and strategic advice on privacy-related matters facing MBIE.</p> <p>Oversight of the Privacy Programme, including delivery of programme initiatives to ensure it is meeting plans and objectives.</p> <p>Agree programme priorities and approve the programme's planned activities to enhance MBIE's personal information</p>

	<p>management capability.</p> <p>Assist the Privacy Officer with decision-making in relation to the programme, including advice and direction to the Privacy Officer to identify and overcome barriers to the successful integration of privacy into business activities.</p> <p>Recommend for approval to the Wellbeing, Health, Safety, and Security Governance Committee components of the MBIE-wide privacy framework.</p> <p>Promote good privacy practices and facilitate engagement with the privacy programme within the members' business groups.</p> <p>Provides leadership in relation to strategic privacy and related matters, (eg information sharing, privacy legislative reform) arising outside of the privacy programme.</p>
<p>Privacy Working Group</p>	<p>Promote the Privacy Policy, standards, and guidance for personal information management.</p> <p>Support the privacy function goals amongst business groups at every opportunity</p> <p>Encourage a positive, learning-from-experience privacy culture at every opportunity</p> <p>Share and discuss examples or elements of good privacy practice developed or undertaken in the business units</p> <p>Identify and raise opportunities for improving privacy-related business processes</p> <p>Provide constructive advice to the privacy programme and function during the development of programme deliverables and function activities</p> <p>Provide an active conduit between the business and the privacy function, including identifying critical business group stakeholders who need to be engaged on privacy matters</p> <p>Report on the business impact of privacy programme initiatives and function activities</p> <p>Oversee the 'lessons learned' process arising from privacy incidents, to ensure rapid dissemination of learnings, and to underpin the development of a positive, learning culture around privacy incidents.</p>
<p>Project Business Owners</p>	<p>Ensure Privacy Impact Assessment Framework is applied to projects in their responsibility.</p> <p>Approve Privacy Threshold Assessments and Privacy Impact Assessments (if required) for projects in their responsibility.</p>
<p>Steward/Owner</p>	<p>Recognised as having the authority and accountability under the policy for the collection of information on behalf of MBIE. The steward defines the information asset requirements of the agency, including ongoing management requirements.</p>

Custodian/Caretaker	Responsible for implementing and maintaining information assets according to the rules set by the steward to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility.
---------------------	--

Procedures

The following business activities support the Privacy Policy by establishing organisation-wide standards for managing personal information and privacy issues:

- [personal information collection](#)
- [personal information requests](#)
- [personal information correction](#)
- [complaints](#)
- [privacy events](#)
- [third party arrangements](#)
- [business process changes](#) (Privacy Impact Assessments)
- staff personal information standard

Business processes and procedures must be consistent with MBIE standards and standard processes for these business activities.

Related MBIE policies and documents

- Code of Conduct
- Security Policy
- Records Management Policy
- ICT Acceptable Use Policy
- Risk Management Policy
- Official Information Act Requests Policy
- Social Media Policy
- Data merging framework
- Inter-agency data sharing framework
- Intra-agency data sharing framework

Relevant legislation and regulations

- Privacy Act 1993 [refer section 6 for the 12 Information Privacy Principles]
- Official Information Act 1982
- Public Records Act 2005

Some legislation provides specific obligations for MBIE in relation to privacy that modify or apply in addition to Privacy Act obligations, for example, the Immigration Act 2009. These must also be considered by managers. For MBIE operations overseas, local privacy laws will also be relevant.

Measures of success

MBIE will measure the success of this policy when it identifies:

- an increase in privacy maturity, as rated by the annual Privacy Maturity Assessment Framework self-assessment and report to the GCPO
- an increase in trustworthiness, as measured by the annual Privacy Survey
- a reduction in harm – as measured by a decrease in customer complaints and negative findings
- that personal information requests are recorded and responded to within legally required timeframes.

Consultation processes in developing or reviewing this policy

This policy was developed as a result of an external review of MBIE's Privacy Programme, where key stakeholders across the organisation were interviewed to determine privacy awareness and planned work.

This policy will be reviewed every three years, or as necessary where there is a significant change in MBIE's strategic direction or organisational responsibilities, or where there is a significant change to the vision for privacy at MBIE or Privacy Programme.

Key stakeholders for consultation on the Privacy Policy include:

- MBIE's Chief Information Officer.
- Head of Protective Security.
- Chief Data and Information Officer.
- Members of the Privacy Working Group.

The Privacy Steering Group will review the Policy, be consulted on any major amendments, and endorse updates to the Policy for approval prior to amendments progressing through policy approval processes under the MBIE *Internal Policy Requirements*.

Compliance management

Compliance management process

The multi-tiered governance arrangements provide oversight of privacy matters, to support compliance with this policy.

Breaches of this policy will be managed through the [Manage privacy event](#) process. These are held in a central register under the responsibility of the Chief Privacy Officer.

Standard processes and guidance issued under this policy will be made available on The Link. Refer to [Privacy processes](#) for more information.

These tools will help ensure compliance with this policy and related mandatory procedures, as well as identifying trends and risks so they can be managed appropriately.

Compliance reporting and information

Compliance information regarding the performance of this policy will be provided to Risk and Compliance on a quarterly basis.

Training and communications

A course providing an overview of privacy at MBIE is available to all staff through Learn@MBIE. Completion of this course is mandatory for new staff and contractors through the *Induction Learning Pathway* and is available for existing staff for on-going 'refresher' training. Courses in security, records management, and responding to information requests also support personal information management practices.

Role-specific training to support staff, contractors and third-party service providers to manage privacy issues arising in their work should be provided by business units.

Policy, standard processes and guidance information is available on the Intranet. The Privacy Programme implements a communications plan that establishes regular communications of key issues via the Intranet and other channels. Where possible, key messages will align with messages from related functions, and/or linked to messages from the GCPO.

RELEASED UNDER THE OFFICIAL INFORMATION ACT