PRIVACY POLICY

Date of Issue	Review Date
01/03/2018	01/03/2019
01/04/2019	31/03/2020
29/06/2020	28/06/2021

Purpose

The Privacy Policy describes for all Agency staff (including contractors) the Agency's expectations on how personal information is managed, who is responsible for personal information, the tasks and responsibilities of those persons, and the tools that are available to support this Policy.

Scope

Part One of this Policy sets out how the Agency manages personal information.

Part Two contains the Agency's requirements for –

- training
- privacy impact assessments
- contractors
- responses to privacy breaches.

Part Three contains the procedures for monitoring compliance through –

- privacy complaints
- audit
- reporting.

Overview

Personal information is information about identifiable individuals. Personal information does not include information about bodies corporate or other organisations.

Personal information is critical to the effective performance of the Agency's functions, both as an employer of staff but also in respect of the Agency's objective to re-enter and recover the drift, and the bodies of any miners found in the drift. The following are examples of personal information the Agency collects and holds –

- information about employees and contractors, such as their dates of birth, home addresses, employment history and medical conditions impacting on their work
- information about the Pike River families.

It is critical that the Agency collects, stores and uses this personal information in a manner that is responsible, legal and transparent. While we have obligations under the Privacy Act as to the way in which we manage personal information, of equal or even greater importance is our desire to establish and maintain a reputation as a credible and competent Agency in whom stakeholders and the public have high levels of trust.

Policy objectives

The Agency's objectives under this Policy are to ensure that –

- we know what personal information we hold
- personal information is managed carefully and consistently, in compliance with our obligations under the Privacy Act 1993
- responsibility for privacy rests not with one individual, but is shared right across the Agency
- every piece of personal information has an "owner" who is responsible for ensuring that the information is managed in accordance with established practices and procedures
- every individual who deals with personal information is clear about their obligations, the expectations on them, and the processes and procedures that are relevant to their work
- we provide training to all staff who require it, and refresh that training regularly
- we manage privacy breaches openly and transparently, and treat every breach as an opportunity to improve our privacy practices.

Help

Should you require help or information about this policy please contact the Chief of Staff, as the Agency's Privacy Officer, for assistance.

Definition of terms

The following definitions are relevant to this Policy

information – is not defined in the Privacy Act but includes –

- written material
- video or audio tapes
- photos
- information stored in computers
- information that is not recorded but is 'held' in the memory of an officer of the Agency.

Information Privacy Principles – means the principles set out in section 6 of the Privacy Act, as explained in Part One of this Policy

personal information – means information about an identifiable person

Key Accountabilities and Responsibilities

Role	Description of responsibility
Chief Executive	Approves this Policy
Chief of Staff/ Privacy Officer	Takes a visible leadership role in the promotion of privacy across the organisation Ensures necessary training is provided to all staff Ensures that the appropriate security measures are in place across the Agency's information system to support the appropriate management of personal information

	Assists others to fulfil their roles and accountabilities Reports to Management Team on – • current privacy issues • breaches and near misses • complaints • investigations Carries out an annual audit of compliance with this Policy
Managers	Ensure that personal information is managed in accordance with the Information Privacy Principles, including ensuring that supporting operational guidelines, processes and procedures (where appropriate) are created, implemented and maintained Ensure that relevant staff understand the Privacy Principles, are familiar with the supporting guidelines, processes and procedures and are putting them into practice Ensure that all staff for whom they are responsible who have access to personal information have received the necessary training provided by the Privacy Officer Work with the Privacy Officer to seek the necessary support and guidance to fulfil their responsibilities
All Managers and staff	Everyone who deals with personal information at the Agency is responsible for the privacy of that information, including – • ensuring they are familiar with the Privacy Principles and understand their obligations in dealing with personal information • following operational guidelines, processes or procedures relevant to managing personal information • taking personal accountability for the appropriate management of personal information to which they have access • maintaining best practice privacy behaviours • promoting privacy at work • actively participating in privacy training • reporting all privacy breaches and near misses to the Privacy Officer • identifying privacy risks.

Related policies and documents

- OIA Policy
- Office of the Privacy Commissioner, "Privacy for Agencies", guidance and further information, available here
- Department of Internal Affairs, Government Chief Privacy Officer, guidance on privacy management, available here.

Relevant legislation and regulations

- Privacy Act 1993, available here
- Office of the Privacy Commissioner, guidance on the Privacy Act 1993 and the information privacy principles, available here.

Measures of the success of the Policy

The success of this policy will be measured by the Compliance Management process establishing that –

- there are no re-occurrences of privacy breaches or near misses
- the annual audit identifies few or no areas of non-compliance with this Policy
- there are no complaints of privacy breaches to the Privacy Commissioner, or if there are complaints the Privacy Commissioner upholds the Agency's decisions or actions.

Consultation processes in developing or reviewing this Policy

This Policy has been approved by the Chief Executive and must be reviewed at least annually to ensure any organisational changes are accounted for.

Compliance Management

To ensure compliance with this policy the Agency will:

- review all complaints and reports from staff of breaches and near misses and take appropriate action to ensure there are no re-occurrences of any such breaches or near misses
- promptly implement the findings of any privacy investigation
- annually review compliance with this Policy
- review and amend this Policy or take other action as appropriate if the Privacy Commissioner does not uphold the Agency's decision on a privacy complaint.

Training and Communication

All staff should have access to this Policy either by being referred to a hardcopy held on site, via the intranet or MAKO (document management system).

Part One – Management of personal information

Information Privacy Principles

Section 6 of the Privacy Act 1993 sets out 12 Information Privacy Principles which govern the way all organisations must gather, store, use and release personal information.

The Agency is committed to acting in accordance with the Information Privacy Principles. The Information Privacy Principles can be accessed here.

Summary of the Information Privacy Principles

Collection (principles 1-4)

The Agency will collect personal information –

- for lawful purposes only
- only when the collection is necessary and related to a function of the Agency.

When the Agency collects personal information, it will, wherever possible, collect it directly from the individual to whom it relates.

When the Agency collects information, wherever practicable, the Agency will advise the subject –

- why the information is being collected
- the purposes for which it will be used
- who will receive and use the information
- the right to access their personal information.

Storage and security (principle 5)

The Agency will ensure that it safeguards personal information it holds against –

- loss
- unauthorized access, modification or disclosure
- any other misuse.

Access and correction (principles 6-7)

The Agency will –

- provide personal information to the individual concerned on request, subject to the provisions of the Privacy Act 1993
- allow for correction of personal information about an individual on request, or allow for an individual's statement to be held alongside the personal information.

Accuracy (principle 8)

The Agency will ensure, prior to using personal information, that the information is up to date and accurate and not misleading.

Retention (principle 9)

The Agency will not keep personal information for longer than is necessary.

Use and disclosure (principles 10-11)

The Agency will generally use personal information only for the purpose for which it was collected,

or for a directly related purpose.

The Agency will not disclose personal information to a third party –

- except in accordance with the Privacy Act 1993
- except on the grounds set out in Privacy Principle 11
- only after seeking legal advice from the Agency's legal advisors.

Unique identifiers (principle 12)

The Agency will only assign unique identifiers when permitted.

Information Security

Agency staff are entitled to access personal information held by the Agency only for legitimate business purposes.

Staff may not access personal information held by the Agency out of personal interest, curiosity, or for any other purpose unrelated to their legitimate work activities.

A breach of this part of the Privacy Policy may amount to serious misconduct and employment action may result as a consequence of any breach.

Information system security

There must be in place across the Agency sufficient information system security measures to prevent –

- unauthorised access by Agency staff to personal information that they have no legitimate business reason to access
- unauthorised access by external third parties to personal information held by the Agency.

Part Two – Requirements for training, privacy impact assessments, contractors, and responses to privacy breaches

Training

Training is an integral element of the Agency's privacy strategy, as it is a mechanism by which to ensure that –

- staff are aware of the overall framework within which personal information is managed at the Agency
- staff understand the basics of privacy law and the obligations the organisation bears in managing personal information
- staff are aware of their responsibilities in managing personal information.

It is Agency policy that –

- all staff who deal with personal information must receive annual training on –
    - the basic requirements of the Privacy Act 1993
    - the Information Privacy Principles and their applicability to the personal information for which they are responsible
    - the Agency's obligations in relation to personal information
    - the privacy framework in place across the Agency
- all staff who deal with personal information must be aware of, and receive training in respect of the procedures and/or operational guidelines relevant to their role.

Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a systematic process for evaluating a proposal in terms of its impact upon privacy. A PIA helps –

- identify the potential effects that a proposal may have upon individual privacy
- examine how any detrimental effects upon privacy might be overcome
- ensure that new projects comply with the information privacy principles.

PIAs may be desirable to assess and address risks –

- arising from a new technology or the convergence of existing technologies, for example, combining face-recognition and CCTV
- where a known privacy-intrusive technology is to be used in new circumstances, for instance, expanding data matching or drug testing, or installing video surveillance in a workplace
- in a major endeavour or change in practice with significant privacy effects, for example, the adoption of new forms of required ID, or shared access to other organisations' electronic data bases.

The Agency must consider performing a PIA when –

- implementing new programmes or systems that involve significant collection, use or disclosure of personal information

- making major changes to existing programmes or systems that involve the collection, use or disclosure of personal information
- undertaking any collection of sensitive personal information in a security context (refer to the Discretionary Expenditure Policy and the State Services Commissioner's model standards for collecting such information).

PIAs should be performed in accordance with the guidance issued by the Office of the Privacy Commissioner, which can be found here.

Contractors

Any Agency staff member who engages external parties under a contract for service must, if the contractor will have access to personal information held by the Agency, ensure that –

- the Agency's expectations as to the management of personal information are written into the contract for service as a legal requirement
- the contractor is made aware of the relevant processes/operational guidelines relating to the management of personal information
- the contractor is given access only to that personal information they require to be able to perform their role
- the contractor acknowledges, in writing, their agreement to comply with Agency policies and procedures/operational guidelines relating to the management of personal information.

Security contractors engaged by the Agency must be expressly prohibited from collecting any sensitive personal information about individuals, in accordance with the Discretionary Expenditure Policy.

Procedures in the event of a privacy breach

A privacy breach is when personal information is inadvertently disclosed to a third party without authorisation.

When a breach occurs the Privacy Officer must be advised as soon as the breach is discovered.

It will be the responsibility of the Privacy Officer to –

- as a priority, immediately contain the breach
- evaluate the risk of harm to individuals associated with the breach
- in light of the assessed risk, take immediate steps to mitigate the effect of the breach. This might include:
    - advising the subject of the information that their personal information has been disclosed, and the steps that are being taken to mitigate the effects of the breach;
    - contacting the recipient of the information and requesting its destruction or immediate return to the Agency;
    - other steps considered appropriate and necessary in the circumstances
- advise the Chief Executive of the breach
- if appropriate, advise the Office of the Privacy Commissioner of the breach (the Government Chief Privacy Officer, DIA, has developed guidance for assessing the scale and severity of privacy breaches and near misses, available here)
- investigate the circumstances of the breach, using the necessary internal or external expertise required given the circumstances of the particular case
- identify the underlying causes of the breach

- identify any training requirements, systems improvements or process/guidelines amendments that could prevent further such breaches occurring
- report to the Chief Executive on the outcome of the investigation, including the recommendation as to required changes. This report must include an analysis of the harm caused to any individuals as a result of the breach, and the risk to the organisation that arises as a consequence.

In managing breaches involving personal information the Privacy Officer must have close regard to the guidelines issued by the Office of the Privacy Commissioner entitled "Key Steps for Agencies in Responding to Privacy Breaches", available here.

Part Three – Monitoring compliance through privacy complaints, audit, and reporting

Privacy Complaints

Any person whose personal information is held by the Agency has the right to complain about the Agency's management of that information.

Any complaints received should be directed to the Privacy Officer.

The Privacy Officer will be responsible for investigating the complaint (in a manner proportionate with the nature of the complaint).

If the investigation reveals a privacy breach has occurred, the appropriate procedures as outlined in this Policy relating to privacy breaches should be followed.

Audit

The Privacy Officer is responsible for ensuring that an audit of compliance with the Privacy Policy is performed on an annual basis.

The audit will be designed to –

- ensure that the appropriate procedures/operational guidelines are being maintained
- ensure that staff are receiving the necessary training in relation to privacy
- review the Agency's practices against the requirements of this Privacy Policy.

The first audit of this Policy (on the first anniversary of the adoption of this Policy) will undertake a Privacy Maturity Assessment in accordance with the Government Chief Privacy Officer, DIA, Privacy Maturity Assessment Framework, available here.

Reporting

The Privacy Officer is accountable to the Management Team for the performance of his/her functions.

The Privacy Officer shall report to the Management Team in relation to:

- any privacy breaches, near misses or complaints reported to the Privacy Officer since the last meeting
- any other privacy-related risks that have arisen since the last report, and the way in which those risks are being managed.

The Privacy Officer shall report annually to the Management Team in relation to the results of the privacy audit.