REANNZ

POLICY STATEMENT

NAME	Privacy Policy
NUMBER	7.1
APPROVAL	Board
POLICY OWNER	Chief Executive Officer

1. PURPOSE

The purpose of this policy is to set out the minimum requirements for the collection, storage and use of personal information by REANNZ to ensure compliance with the Privacy Act 2020 and other relevant laws.

2. SCOPE

This policy applies to all REANNZ Employees, Officers, Contractors, Interns and Consultants.

This policy applies to all personal information relating to an individual collected, stored, disclosed and used by REANNZ, including but not limited to Employee information, Customer and Member information, Supplier information and Network Information.

3. POLICY STATEMENT

REANNZ's collection, storage, disclosure and use of personal information will be undertaken in accordance with the Privacy Act 2020, and the Public Services Commission's model standards for information gathering (see Appendix)

REANNZ will:

a) collect personal information directly from the person concerned unless there are legitimate reasons not to (e.g. the information is publicly available)

b) be transparent about what information is collected and how it will be used by REANNZ

c) collect no more than the minimum amount of personal information necessary to achieve the purpose for which the information is required

d) ensure the information collected is stored securely

e) actively manage access to and use of the personal information it holds to protect the privacy of individuals

f) keep personal information for the period of time required by law

g) ensure that individuals or their authorised representatives are able to exercise their privacy rights and have some control over their information if they think it is incorrect.

h) Inform the Office of the Privacy Commissioner as soon as practicable of any breach of privacy that has caused serious harm to someone (or is likely to do so).

i) Ensure a REANNZ Privacy Officer is able to oversee compliance with the requirements of the Privacy Act 2020 and manage any breaches of privacy or complaints.

4. RESPONSIBILITIES

The Chief Executive is REANNZ's nominated **Privacy Officer**. The primary role of the Privacy Officer is to encourage the organisation's compliance with the privacy principles and provisions of the Privacy Act 2020. The Privacy Officer will also manage any privacy breaches including any requiring escalation to the Privacy Commissioner, deal with personal information requests (PIRs) and manage any other issues concerning personal information generally.

All REANNZ staff members must:

Understand and comply with the Privacy Policy

Actively participate in any Privacy Training provided by REANNZ

Inform the Privacy Officer of any privacy breaches, PIRs or any other privacy issues:

5. DEFINITIONS

"Personal Information" is any information that tells us something about a specific individual. Information can include personal information such as notes, emails, recordings, CCTV footage, staff performance information, correspondence, opinions photos and scans, whether they are in hard copy or electronic form.

6. EMPLOYEE INFORMATION

REANNZ will only collect and hold personal information about Employees that is relevant to the person's employment with REANNZ.

Information about an individual's employment with REANNZ will be held in a personnel file. These files may be held in a number of places in electronic or hard copy format. REANNZ will take all practical steps to ensure that access to personnel files and the information they contained is only accessible by:

a) The Employee concerned

b) The Employee's manager

c) The Chief Executive

d) Appropriate staff in the Corporate team for the purposes of processing payroll and maintaining accurate employee records.

Information about Employee's computer, internet, email and phone use may be collected in line with REANNZ 5.8 Information & System Security Policy.

7. NETWORK USER'S INFORMATION

REANNZ collects data relating to use of the network ("network information") as part of prudent business

practice for the purpose of monitoring and improving network performance, measuring network performance and usage, troubleshooting network issues, performing network diagnostics, network management, network security and for reporting network usage and trends.

REANNZ will only use services holding data within similar jurisdictions safeguards as NZ and will ask expressly for individuals consent otherwise.

As a general rule, personal information relating to an individual is not collected as part of network measurement activity.

All Network information collected will be in accordance with the 8.3 Network Measurement Policy.

8. ACCESS

Individuals may access information held about them in accordance with Principle 6 or the Privacy Act 2020

A PIR must be dealt with as soon as reasonably practicable, and not later than 20 working days after the date on which the request was received, unless an extension is necessary due to the large quantity of information sought or the need for extensive consultation regarding the request.

9. USE & DISCLOSURE

REANNZ must take reasonable and practical steps to ensure that personal information is up to date, accurate, relevant and not misleading before using it.

Information collected from a person by REANNZ for one purpose should only be used for that purpose.

In the event that REANNZ wishes to use personal information in new ways, it will seek the authorisation of the person concerned or their authorised representative.

Before sharing information with a contracted service provider or overseas recipient, REANNZ will ensure that the service provider or overseas recipient is able to provide appropriate jurisdictions safeguards as NZ in relation to information shared.

10. COMPLAINTS & BREACH

A breach of one or more of the privacy principles by REANNZ is interference in the privacy of the individual and gives rise for complaint if the breach is likely to negatively affect the individual.

Employees, Officers, Contractors and Consultants should notify the Privacy Officer immediately if they become aware of or suspect that a breach of privacy has occurred.

The Privacy Officer will investigate the breach, in line with the contain, assess, notify and prevent approach set out in the Privacy Commissioner's Privacy Breach Guidelines(see Appendix),

Any breach of privacy which has or is likely to cause serious harm must be reported to the Privacy Commissioner as soon as practicable to do so through the Privacy Commission's NotifyUs process (the online guidance can be found here: https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/).

Deliberate breaches of the privacy of personal information held by REANNZ will be treated as a disciplinary matter.

11. REFERENCES

- Privacy Act 2020

12. RELATED POLICIES

Related policies that may impact on, or be impacted by, this policy:

- REANNZ 5.8 Information & System Security Policy
- REANNZ 8.3 Network Measurement Policy
- Website privacy statement

13. APPENDICES

Appendices to follow:

- Information gathering and the public trust (State Services Commissioner)
- Responding to privacy breaches (Privacy Commissioner)

Document version control		
Policy Reference	7.1	
Status	Approved	
Written by / (Owner)	CEO	
Approved by	Board	Via Audit and Risk Committee
Review period	Three years	Next review November 2023

Version History

Version	Date	Reviewed / Approved By	Purpose/Change
2.0	Nov 2012	HR Committee	Substantive rewrite
2.0	Dec 2012	Board	Approved v2
2.1	July 2014	Audit Committee	Minor edits.
2.1	August 2015	Audit Committee	Minor edits
2.2	September 2018	Management	Minor Edits – no policy change
2.2	April 2019	Management	Added reference to new SSC model standards in information gathering
3.0	November 2020	Management	Changes to reflect 2020 Privacy Act

ACTING IN THE SPIRIT OF SERVICE

Information gathering and public trust

Model standards for information gathering associated with regulatory compliance, law enforcement and security functions. Effective from 18 December 2018.

STATE SERVICES COMMISSION
TE KAWA MATAAHO

> Public servants must be vigilant in how they exercise the significant responsibilities and powers entrusted to them by New Zealanders. This is fundamental to the integrity of the public service. Government agencies must ensure that the way they use their authority to collect information is not only lawful, but supports public trust.
>
> — Peter Hughes, State Services Commissioner

Government agencies collect a wide range of information in order to carry out their responsibilities. This information falls into two broad categories:

- Information necessary to deliver functions and services to New Zealanders and businesses
- Information needed to give effect to the responsibilities agencies have to protect people, information and places, to ensure regulatory compliance, and to detect and prevent criminal offending.

These model standards provide a set of expectations for the second category of information.

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 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.

State sector agencies should use these standards when establishing or reviewing their policies and practices in this area.

SCOPE OF THE STANDARDS

There are two key elements to these standards:

1. Legislative and policy framework: ensuring that agency policies provide an appropriate framework for information gathering.

2. Organisational safeguards: ensuring that agencies have appropriate safeguards in place.

LEGISLATIVE AND POLICY FRAMEWORK

Ensuring public servants' actions are lawful

Agencies ensure that their information gathering is lawful.
This includes compliance with:

- any agency-specific legislation
- the Privacy Act 1993
- relevant court decisions
- the New Zealand Bill of Rights Act 1990
- the Search and Surveillance Act 2012.

Agencies take particular care in relation to information gathering associated with regulatory compliance, law enforcement and security functions to ensure that:

- There is a clear purpose and necessity for the information gathering and the information gathering is lawful.
- The information gathering (both the type of information and the way it is collected) is proportionate and reasonable.

Model standards:

- Agencies take the following into account in their policies, and when making decisions about information gathering:
  - Any agency-specific legislation.
  - The Privacy Act 1993.
  - Any guidance issued by the Government Chief Data Steward, Privacy Commissioner or Ombudsman.
  - Relevant decisions by the courts.
- Agencies also take into account the obligations on public servants under the State Services Commission's Code of Conduct, which mean that some ways of gathering information that are lawful for private citizens to undertake are not appropriate for public servants.
- Agencies that undertake information gathering for regulatory compliance, law enforcement and security purposes pay particular attention to the following:
  - The protection against unreasonable search and seizure in the New Zealand Bill of Rights Act 1990.
  - The Search and Surveillance Act 2012.

Ensuring public servants act in accordance with the State Services Code of Conduct

The State Services Commission Code of Conduct sets out expectations of public servants that are designed to retain public trust and confidence. It is supported by agency codes.

New Zealanders expect that public servants carry out their work in a way that is lawful and reasonable, respects individuals' rights to personal privacy, and other rights, including the right to freedom of expression, freedom of peaceful assembly and freedom from unreasonable search and seizure.

Model standards:

- For the avoidance of doubt, it is not acceptable for an agency to:
  - Classify a person or group of people as a security threat - and to use that as justification for gathering information - solely because they lawfully exercise their democratic rights (including their right to freedom of expression, association, and peaceful assembly to advocate, protest or dissent)
  - Gather information about people or groups for the sole purpose of managing reputational risk to an agency.

This requires public servants to ask both: Can we lawfully gather and use this information, **and** should we?

ORGANISATIONAL SAFEGUARDS

Agencies have organisational safeguards in place to support information gathering activities for regulatory compliance, law enforcement and security functions; for example in investigating fraud, tax evasion or another activity of a criminal nature, or where there is suspicion that a person has attempted to deceive or mislead the agency.

The robustness of these safeguards is critical to supporting public trust and confidence where monitoring and surveillance activities are being considered to gather information (for example to support an investigation or prosecution).

Implementing strong and comprehensive policies and processes

It is most appropriate for Parliament, or Responsible Ministers where the law allows, to set the boundaries (in legislation or policy) for these activities when conducted by government agencies, given the competing interests in public safety and in individual privacy that are associated with information gathering activities.

Note that intelligence and security agencies have their own surveillance and information gathering policy frameworks as specified in legislation.

Supporting processes require appropriate signoffs of decisions by agency legal teams.

Model standards:

- Agencies have policies and operational processes in place that describe:
  - the agency's mandate to undertake information gathering activities
  - the scope of activity within that mandate
  - the decision-making framework and process that staff should follow when considering such activity, including when a warrant should be sought
  - relevant legislation, case law, and standards (context specific)
  - the support or training provided to staff
  - review, accountability and oversight mechanisms
  - guidance on the use, storage and destruction of any information collected.
- Agencies regularly review their legislation and policies to ensure that they provide an appropriate framework for regulatory compliance and law enforcement activities and provide advice to Ministers accordingly. The review should include completion of a Privacy Impact Assessment.

Agencies that collect information for regulatory compliance, law enforcement or security purposes ensure that their policies cover the range of information gathering activities undertaken, so that staff are well supported, and governance is effective.

An agency can compile its information to carry out analysis that supports risk assessment and targeted compliance management or enforcement actions, provided information has been gathered lawfully and is consistent with the original purpose for collection.

Policies also outline protocols for managing information gathered by third parties

Model standards:

- Agency policies are specific about the protocols that apply to information gathering for risk assessment, compliance management or enforcement purposes (for example: what sources are appropriate and why; how information is collected and analysed, how information will be stored).
- Agency policies are clear about what steps are taken to verify information sources and validate the information source, where appropriate.
- Information provided to agencies that appears to have been obtained illegally is reported to New Zealand Police.
- Policies and training support staff working in these areas to understand and navigate the important issues of professional distance and public perception associated with the exercise of their powers.

and provided to agencies, including protocols for managing unsolicited information received from known or anonymous sources.

Policies include the expectation that staff will not condone information gathering which is illegal, or inconsistent with the Code of Conduct.

Operational policies, training, and leadership culture support public servants working in regulatory enforcement, legislative compliance and security functions to understand and safely navigate issues such as professional distance when undertaking information gathering, monitoring and investigation activities.

Publishing a transparency statement

Agencies are transparent with New Zealanders about the kind of information gathering activity that they undertake (in both physical and digital environments) and the purpose of that activity.

This will be specific enough to be meaningful for the public, and enable people to understand what the information might be used for, what steps the agency may take to collect it, and in what circumstances. Where agencies already publish privacy statements that meet this purpose, the information does not need to be repeated.

If an agency would have grounds to withhold the information under the Official Information Act 1982, then that information would not need to be included.

Model standards:

- Agencies publish general information about the type of information gathering activity they undertake and the purpose of that activity as a transparency statement.
- Agencies publish their transparency statement on their websites.

Putting in place clear and robust governance arrangements

There are well-defined governance arrangements and decision-making accountability across information gathering for these functions.

These work well when accountabilities for decisions about information gathering are clearly defined and senior leaders have enough information about what is proposed to happen in practice on the ground, and why, to exercise due diligence and ensure that staff are being supported.

Model standards:

- Agencies have well-defined governance arrangements and decision-making accountabilities across the regulatory compliance and enforcement functions. Governance has a specific focus on information gathering activities.
- Governance arrangements include a requirement to seek advice from agency legal teams, and Crown Law, when appropriate.

Ensuring rigorous review and oversight

Explicit review and oversight of information gathering provides robust assurance that the expected standard is being met. The nature of this oversight will be determined by the context and functions of the agency, and will be part of normal governance arrangements.

For some agencies with significant and potentially intrusive information gathering powers, Parliament has already determined that oversight will be exercised through a separate independent authority. For example, the Inspector General of Intelligence and Security oversees actions undertaken by New Zealand's intelligence and security agencies.

Model standards:

- Explicit review and oversight of information gathering activity is in place to ensure compliance with the law, policy, and agency risk management requirements.
- Regulatory compliance and law enforcement functions have an oversight arrangement (e.g. by an individual or group not directly involved in the investigation function) to provide assurance the expected standard is being met.
  - The oversight function is charged with reviewing governance and accountabilities, policies and processes and how these translate into practice in specific cases on the ground. Part of their role is to recommend improvements in any of these areas.
  - The oversight arrangement has direct access to senior leadership and the agency's Risk and Assurance Board or Committee to report any concerns.
  - Agencies publish reports from the oversight individual or group about how the oversight function works.

Establishing fair and effective complaints or review processes

Most agencies will already have internal complaints procedures and channels that serve this purpose. External complaint mechanisms are provided through the Office of the Privacy Commissioner, the Office of the Ombudsman, or a similar public body.

Model standards:

- There is an effective complaints or review process in place.
- Complaints or review processes are tied directly to functions where concerns about information gathering activities may arise.
- Information about how to make a complaint or ask for a review is linked to an agency's transparency statement.

WORKING TOGETHER

There are a number of situations where public servants operating under different legislative authorities work together to achieve outcomes. For example, regulators coordinating enforcement action (either across or within agencies), or agencies working together to manage a security threat.

Strong working relationships between agencies can produce better outcomes and faster responses (For example, to new compliance issues). Formal agreements about the use of powers, information sharing protocols and decision-making give the public confidence that powers are being used appropriately.

Joint governance should be in place ahead of delivery, including clearly assigned lead accountability for ensuring the agreed arrangements are effective and align with these standards.

HEALTH, SAFETY AND SECURITY

Agencies will have security plans in place that detail protocols for responding to threats to the safety of staff and customers, including referring incidents to New Zealand Police (unless the agency has specific powers and/or capability to address such threats).

In determining what steps are reasonably practicable to address health and safety issues that involve physical security threats to staff and customers, agencies need to take appropriate advice and demonstrate due diligence. In line with these standards they should consider not only what steps are legal, but also what is ethical, and seek advice where appropriate.

USE OF EXTERNAL SECURITY CONSULTANTS

External security consultants may be engaged by government agencies to assist with information gathering, for example in relation to carrying out risk analysis when there is a serious threat to staff safety. 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.

Model standards:

- Agencies have specific policies governing the use of external security consultants.
- External security consultants are not used to undertake information gathering that would not be lawful and ethical for the agency's own staff to undertake.

Use of third parties is not a way to contract out of legal requirements and the State Services Code of Conduct – agencies should expect the same behaviours from contractors working on their behalf, as they do of their own staff. Compliance with the Code should be a term of any contract.

The task or service should be well-defined through a contract regardless of the scale of engagement. Robust contracts include specific protocols around any information management aspects, including compliance with the Public Records Act 2005, Official Information Act 1982, and the Privacy Act 1993.

Where government agencies do decide to use external security consultants, it is good practice to support this with strong governance and information management practices, and a culture that guides staff in understanding the issues to be careful of when they are working with these firms. A robust procurement process is essential, including assurance that suppliers and any subcontractors have the necessary licenses; are compliant with the Private Security Personnel and Private Investigators (Code of Conduct - Surveillance of Individuals) Regulation 2011; and that conflicts of interest are declared and managed appropriately.

SYSTEM SUPPORT

System support is available to help government agencies navigate these issues:

- Consult the Government Chief Privacy Officer's team in DIA on privacy issues.
- The Government Chief Data Steward supports agencies with guidance on the safe and effective use of data and analytics.
- Your agency's legal team should be consulted for legal advice, and the Crown Law Office can also provide legal assistance. Crown Law can be contacted through your agency's legal team.
- The Government Regulatory Practice Initiative (G-REG) provides support for actions that improve regulatory practice, leadership and capability. SSC and G-REG will jointly host sessions for agencies to discuss these model standards.
- NZ Police should be contacted in relation to serious and specific security threats (unless the agency has specific powers to address such threats). In addition, where agency protocols have escalated an issue to your national level executives, contact the Assistant Commissioner: Investigations at Police National Headquarters.
- The Government Health and Safety Lead can assist with health and safety issues.
- In addition to the NZ Police, the Government Protective Security Lead, working through the Protective Security Requirements (PSR) team, can assist agencies in responding to serious security threats. Agencies can seek support and test their thinking with the functional lead through their PSR contact, or at psr@protectivesecurity.govt.nz.
- The Ministry of Business Innovation and Employment provides procurement advice and supports the Protective Security Panel in conjunction with the PSR team.