



23 June 2025

Tēnā koe

Official Information Act Request

Thank you for your email of 1 May 2025, requesting information regarding Regional Health Officers, the amount of funding spent on adult safeguarding teams engaged by Disability Support Services (DSS), and policies on the Ministry of Social Development's (the Ministry) handling of client information.

I have considered your request under the Official Information Act 1982 (the Act).

- 1. Is the role of regional health officer at MSD DSS and MSDWINZ the same as the medical professional advising the review panel at MSD DSS?*

I can confirm that the medical advisory role for the Review Panel is a separate role from the regional health officer role within Work and Income. These roles do not have any overlap in terms of responsibility.

- 2. I would like to know how much funding has been allocated to adult safeguarding teams engaged by MSD DSS in the last five years and how much went to individuals for the purpose of making a life changing improvement that could prevent abuse in all forms.*

In 2023–2024 DSS contracted for the prototype and delivery of Safeguarding Adults Specialist Support with a funding amount of \$2.46 million. This contract for services, now referred to as Disability Abuse Prevention and Response (DAPAR) services was extended into 2024–2025 with a funding amount of \$2.2 million and comes to an end on 30 June 2025.

Currently there is a procurement process underway to contract for delivery of safeguarding services for the period 1 July 2025 to 30 June 2027. This process is not yet complete. More information on DAPAR services can be found here:

- www.disabilitysupport.govt.nz/providers/quality-and-safeguarding/disability-abuse-prevention-and-response

I am refusing your request for the amount of funding which went to individuals for the purpose of making a life changing improvement that could prevent abuse under section 18(g) of the Act. The information you request is not held by the Ministry, and I have no grounds to believe that the information is either held by or closely connected to the functions of another department, Minister of the Crown or organisation.

3. *So, my third question is, can I please have a copy of the information used to define the service interface between Health, Disability, Justice and Mental Health. How does DSL or any NASC define this and by the use of what tools? The operational policies state that multiple funding can use an existing interface but is this available through an EGL office and if not, how can it be accessed on an independent basis? What assessments are used, and can this be arranged privately along with private intensive service facilitation? Is there a policy or procedure that details how to action the use of these assessments?*

You can find the Health New Zealand Service Coverage Expectations 2024-25 document through the following link:

- https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.health.govt.nz%2Fsystem%2Ffiles%2F2024-08%2Fservice_coverage_expectations_24-25_july_24.docx&wdOrigin=BROWSELINK

This document outlines the range of services funded for eligible people by Health New Zealand as well as other specified health entities and agencies which includes DSS.

I have interpreted the second section of question 3 to mean whether funding provided by other agencies could be accessed through an EGL site. I can confirm that an EGL site would only be able to provide funding for any disability supports and any additional supports required. For other services, then people would need to access those through the relevant agency.

4. *Please provide a copy of any policy MSD DSS or MSD WINZ has for the handling of individual health information.*

I have attached the following Ministry policies below which relate to client information:

- Privacy, Human Rights and Ethics Policy.
- Information Security Policy.
- Information Governance Policy.

You can also find further information about how the Ministry handles personal client information here:

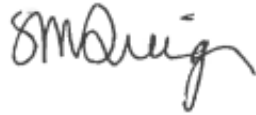
- www.workandincome.govt.nz/about-work-and-income/privacy-notice/index.html

I will be publishing this decision letter, with your personal details deleted, on the Ministry's website in due course.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with my decision on your request regarding Disability Support Services, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

pp. 

Anna Graham

General Manager
Ministerial and Executive Services

Information Security Policy

Last Review Date:	November 2024
Next Review Date:	November 2026
Approved by:	Organisational Health Committee
Owner:	General Manager Information (CISO)

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) in upholding its Information Security responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for Information Security. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's information culture and decision-making.

Policy Statement

The Ministry holds and uses information and data about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

Robust information security is a fundamental business enabler. The Ministry relies on the confidentiality, integrity, and availability of the information it holds and uses to maintain the trust and confidence of the New Zealand Government and public. The Ministry has a responsibility to keep information assets safe and available to those who need it; and reduce the risk of information loss, damage, or compromise.

Scope

This policy applies to all Ministry staff including contractors; all information held and used by the Ministry (physical and electronic); and all activity conducted by third parties on behalf of the Ministry.

There are unique roles at the Ministry which cover the roles for information security as described in the New Zealand Information Security Manual (NZISM). Refer to Roles and Responsibilities for a description of these roles for the Ministry.

Policy Principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry protects information assets through right-sized security controls

The Ministry takes a risk-based approach for the protection of information assets. We assess the value and priority of potential threats and identify actions to reduce risk to acceptable tolerances. The Ministry's standards form the mandatory baseline for how we securely design, build, implement, manage, and use our systems and information assets. The application of these standards is dependent on the nature of the information, system, service, or business process. Where a Ministry standard does not exist, we follow applicable guidance from the NZISM.

2. All changes made to Ministry systems and their configurations are developed, tested, and applied in a secure and timely manner

The Ministry creates and collects, stores, and uses information across IT assets and services which will continuously need to undergo change to remain secure, stable, and scalable. To limit exposure of security risks to Ministry technology and information, all changes are tested in a pre-production environment, follow secure design lifecycle (SDLC), operate on supported software versions, and undergo certification and accreditation and testing when appropriate.

3. Ministry IT systems are continually logged and monitored for threats and vulnerabilities to ensure security risks are well-managed

The Ministry proactively monitors its IT environment to detect and respond to security events in a timely manner. Security risks are reported to accountable parties and inform operational decisions and priorities. Security events and alerts are triaged and, if appropriate, security incidents are raised to track and manage. When security incidents occur, the Ministry takes all necessary steps to contain and eradicate threats and recover systems in a coordinated manner and in line with legislative and standard requirements.

4. Access to and use of Ministry information is only available to those that need it to perform their role

The Ministry recognises data and information as taonga and uses an information classification process to determine and assign the required level of protection and access. An authenticated identity permits access to, and use of, Ministry-held information based on assigned privileges. These permission levels are based on the minimum needed for a person to perform their role.

5. Ministry IT systems and information assets can be recovered and restored within acceptable timeframes and levels

The Ministry understands its emergency management and business continuity responsibilities for information and ensures it can meet availability and recovery requirements following adverse events. Business continuity and disaster recovery plans are regularly assessed to ensure Ministry IT services and Ministry-held information can be recovered.

Roles and Responsibilities

The table below details the roles specifically required to establish governance across Information Security as described in the NZISM – Chapter 3:

Role (NZISM)	Responsibility
Chief Executive	<p>The agency head who is accountable for information security within their agency.</p> <p>Where the agency devolves their authority, the delegate must be at least a member of the Senior Executive Team or an equivalent management position.</p> <p>At MSD, the Chief Executive role has been delegated to the Chief Security Officer (CSO), who is also the DCE of Organisational Assurance and Communication (OAC).</p>
Board of Directors	<p>Accountable for organisational governance. Provides strategic direction and communicates the organisation's cyber security principles by:</p> <ul style="list-style-type: none"> - Setting the strategic security direction of MSD - Assisting prioritisation by helping to identify critical assets and highlighting key risks - Assessing the effectiveness of the cyber security strategy. <p>At MSD, the Board of Directors is the MSD Leadership Team (LT).</p>
Executive Management	<p>Responsible for ensuring the implementation of the cyber security strategy; providing resourcing to deliver, approving policies and standards, and measuring the effectiveness of the cyber security programme.</p> <p>At MSD, the Executive Management team is the Leadership team, and its two delegated committees, the Transformation and Investment Committee, and the Organisational Health Committee.</p>
Chief Information	<p>The CISO sets the strategic direction for information security within their agency. The CISO is responsible for cyber security requirements, and accountable for representing cyber security,</p>

Role (NZISM)	Responsibility
Security Officer	<p>leading a programme of cyber security continuous improvement & managing a virtual team through a distributed security function.</p> <p>The Chief Executive (CE) has delegated the MSD CISO role to the General Manager (GM) Information. The GM Information is responsible for implementing and having assurance over this policy.</p>
Information Technology Security Manager	<p>The ITSM provides information security leadership and management within their agency.</p> <p>At MSD, the delegated ITSM is the Director Technology Security and Identity.</p>

The following table details the teams, groups, and bodies which collectively play an important role in governing information security for the Ministry of Social Development:

Group	Responsibility
Information, Security and Identity Group	<p>The Information, Security and Identity Group is responsible for:</p> <ul style="list-style-type: none"> • Supporting MSD's strategic future – providing thought leadership on information security, privacy and information management across, as well as influencing information maturity growth across MSD and all of government • Delivering assurance - providing support to MSD in meeting its compliance responsibilities through an assurance programme to manage defined information risks. • Providing expert advice - providing specialist skills to ensure business processes and systems design align to good practice, including responsible use and protection of

Group	Responsibility
	<p>information assets and comply with information legislation and related regulations.</p> <ul style="list-style-type: none"> • Delivering a foundational capability - providing direction, guidance tools, training and support for information capability improvements. <p>Technology Security and Identity is responsible for MSD's Technology Security and Identity Operations. This covers the following Information Security responsibilities:</p> <ul style="list-style-type: none"> • Developing, implementing, and monitoring security technology • Enforcing operational procedures and hardening systems and configurations • Remediation of risk to business systems and applications • Ongoing assessment and review of cyber threat intelligence sources • Oversight and management of vulnerability scanning, analysis, and remediation • Management of security in the operating environment on a day-to-day basis • Management of security incidents and response actions • Monitor's anomalies and trends in security technologies • Approves security changes in change advisory/control boards • Reports on exceptions to IT Security owned standards • Privileged access monitoring and approval of privileged user accounts provisioning
Improvement Systems and Technology (IST) Group	<p>IST is responsible for enabling people and partners with improved services and effective technology so New Zealanders can easily access the support they need.</p> <p>IST is part of the Transformation Group and are made up of service improvement and technology experts, including Technology Security and Identity.</p>

Definitions

Word/ phrase	Definition
Authenticated Identity	The outcome of a process which has proven that a person or entity is who they say they are.
Availability	Data availability means that information is accessible to authorised users. It provides an assurance that your system and data can be accessed by authenticated users whenever it is needed.
Confidentiality	Confidentiality ensures that information is accessed only by an authorised person and protected from unauthorised disclosure. It is implemented using security mechanisms such as authentication, passwords, access controls, and encryption.
Information Assets	An Information Asset is an identifiable collection of information and data recognised as having value to the agency. Information assets can be physical or electronic. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Management	Information Management is the process by which MSD ensures that information is managed across its lifecycle, such that it is accurate, relevant, and accessible; and that it is retained and disposed of appropriately in line with its value and its risk profile. There is an obvious overlap between information security, information management and privacy. Information Management is not covered by this policy; rather this policy recognises the interdependence of one to the others.
Information Security	Information Security relates to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".
Integrity	Integrity refers to the accuracy and completeness of data. Security controls focused on integrity are designed to prevent data from being modified or misused, either deliberately or accidentally.
Privacy	Privacy relates to the rights you have to control your personal information and how it's used. There is an obvious overlap between information security, information management and privacy. Privacy is not covered by this

	policy; rather this policy recognises the interdependence of one to the others.
--	---

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Information Governance Policy

Last Review Date:	November 2024
Next Review	November 2026
Date:	
Approved by:	Organisational Health Committee
Owner:	General Manager Information (CISO, CPO)

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) in upholding its Information Governance responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for Information Governance. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's Information culture and decision-making.

Policy Statement

The Ministry holds and uses information (including personal information and data) about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

Effective information governance requires the Ministry to understand the information it holds, define who is responsible for that information, and know how that information is being used. Additionally, it requires the Ministry to have assurance that its information is protected, is managed appropriately, and its staff are acting responsibly when using information.

Scope

This policy applies to all Ministry staff including contractors; all information and data held and used by the Ministry; and all activity conducted by third parties on behalf of the Ministry.

Policy Principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry's information assets are identified and appropriately protected based on legislative requirements, information value and risk culture

The Ministry manages information assets in accordance with the requirements defined in key legislation such as the [Public Records Act 2005](#), [Privacy Act 2020](#), and the [Official Information Act \(1982\)](#), along with policy guidance such as the [Protective Security Requirements](#) (PSR). The Ministry's standards and other guardrails define the measures which set the baseline for how information assets are collected, secured, stored, used, and managed using a risk-based approach.

2. All information assets held by the Ministry have responsible Information Asset Owners to ensure they are managed and used appropriately

An information asset has value to the Ministry from the point of creation or collection through to its eventual disposal. Information Asset Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are understood, managed and monitored throughout the information asset's lifecycle. Information Asset Owners are also responsible for how their information assets are used, including use with algorithms or other tools. Any legal and regulatory requirements applicable to the collection, storage, use, disclosure or disposal of the information must be understood by the Information Asset Owner.

3. Information assets are fit-for-purpose to promote informed decision-making

Consistently and continuously maintaining the quality and integrity of Ministry information assets ensures people use authoritative information. The information collected, used, and shared by the Ministry is appropriate for the purposes it is intended and collected for, and contributes towards better insights, better decisions, and better lives.

4. The Ministry partners with tangata whenua in decision-making about information held by the Ministry to support Māori

The Ministry fosters collaborative relationships with Māori communities to ensure their voices are heard and respected in decisions about information held by the Ministry that impacts their lives. The Ministry values the trust placed in it by Māori and is dedicated to embedding Māori perspectives into the way it cares for and manages Māori information. Upholding its responsibilities to its Accord partners, the Ministry is committed to working alongside key partners to support decisions about how Māori information is governed.

5. The protection and responsible use of Ministry information is everyone's responsibility

Ministry staff are responsible for handling information appropriately while it is in our care. Ministry technology and processes play a key role in providing a layer of protection over information, and our awareness of information risk and its acceptable use is just as important. The Ministry expects staff to act in a timely and coordinated manner to prevent or respond to breaches of, and threats to, information.

Roles and Responsibilities

Everyone that works for or is contracted to the Ministry has a responsibility to comply with this policy. The responsibility of each role specifically relevant to this policy is set out in the table below:

Person/Party	Responsibility
All Staff	<p>All staff are responsible for:</p> <ul style="list-style-type: none"> • Complying with the Ministry's information policies • Following information guidance and training • Identifying and reporting information security, information management, and privacy incidents • Escalating risks, as needed, to their manager
Managers	<p>All managers are responsible for:</p> <ul style="list-style-type: none"> • Leading and facilitating regular information discussions with their teams • Ensuring their teams are familiar with the Ministry's information policies and guidance; use approved tools, and comply with the Ministry's information governance approach • Providing direction on acceptable behaviours to their teams • Modelling good information practice through their actions and behaviour • Identifying and escalating information risks, as appropriate, to ensure information is managed effectively at the appropriate level and in a timely way • Reporting any information security or privacy incidents to their line manager

Person/Party	Responsibility
Information Asset Owners	<p>All information assets owners are responsible for:</p> <ul style="list-style-type: none"> • Leading and championing a culture that values protection and responsible use of information; • Understanding which information assets, they are accountable for, their value, where they come from, and how they are used; • Knowing who has access to that information and why and ensuring that access is controlled and reviewed continuously; • Ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored; and • Ensuring their information assets are fully utilised in line with responsible information use. <p>The information asset owner must understand the value of each information asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information asset.</p> <p>At the Ministry, Information Asset Owners will typically be assigned at the Tier 3 senior leader level, reporting directly to Deputy Chief Executives (DCEs).</p>
Information Stewards	<p>Information Stewards are responsible for:</p> <ul style="list-style-type: none"> • Maintaining specialist knowledge about the information in their business area. • Ensuring information is available for its intended purpose; • Managing and maintaining information assets based on MSD standards, policies, and other guardrails, including data quality, integrity, and metadata; • Maintaining and updating an inventory of information assets; • Monitoring and optimising the lifecycle of information to effectively manage risk and opportunities; • Collaborating with stakeholders across the business (System Owners, other Information Stewards, Business

Person/Party	Responsibility
	<p>Capability owners, and Line 2 assurance functions, etc.) to implement the necessary guardrails;</p> <ul style="list-style-type: none"> • The responsible use of information assets, enabling the organisation and other agencies where appropriate to gain maximum value from the information; and • Supporting information asset owners to make informed decisions about the management and use of their asset for the duration of its lifecycle. <p>The Information Steward must keep the Information Asset Owner informed and aware of any risks or concerns surrounding the integrity or safety of the information.</p> <p>At the Ministry, Information Stewards will be assigned by the Information Asset Owners and are typically senior subject matter experts in their respective business areas.</p>
Information Governance Committees	<p>Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance. They set the overall risk culture for the Ministry, which guides the way it responds to information risk and opportunity.</p> <p>These governance bodies must have membership from the Ministry's Leadership Team, as well as appropriate Māori representation, and have oversight of:</p> <ul style="list-style-type: none"> • Information and IT security policies and strategies • Information standards and architecture • Obligations contained in the Protective Security Requirements (PSR), the Privacy Maturity Assessment Framework (PMAF), and the Archives New Zealand Information and Records Management Standard • Ministry decisions about ensuring there are adequate systems, processes, and controls in place to identify and manage information risk. <p>At the Ministry, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC), the Information and Protective Oversight Committee (IPSOC), the Transformation and Investment Committee, and Tai Nuku Design Committee.</p>
Executive Sponsor Information	<p>The Executive Sponsor champions the importance of information management among the organisation's leadership. The aim is for everyone in the organisation to see information management as an integral part of a business operating</p>

Person/Party	Responsibility
	<p>effectively. The Executive Sponsor Information is responsible for:</p> <ul style="list-style-type: none"> • Ensuring that the strategy and policy adopted by the organisation supports information management • Being involved in strategic and operational planning to align information management with the corporate objectives and business activities of the organisation • Liaising with business units to ensure that information is integrated into work processes, systems, and services • Overseeing the budget for information and ensuring the resources needed to support information are known and sought in funding decisions • Ensuring that staff with appropriate skills to implement information strategies are employed, and regular upskilling is available • Monitoring and reviewing information to ensure that it is implemented, transparent and meets business needs <p>The CE has delegated the Executive Sponsor Information role to the DCE Organisational Assurance and Communication (OAC).</p>
Chief Security Officer	<p>The Chief Security Officer (CSO) is responsible for having oversight of the Ministry's protective security practices in line with Protective Security Requirements (PSR).</p> <p>At the Ministry, the CSO is the DCE OAC.</p>
Chief Information Security Officer	<p>The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency. The CISO is responsible for cyber security requirements, and accountable for representing cyber security, leading a programme of cyber security continuous improvement, and managing a virtual team through a distributed security function.</p> <p>At the Ministry, the CISO is the General Manager (GM) Information. The GM Information is responsible for implementing and having assurance over this policy.</p>

Person/Party	Responsibility
Chief Privacy Officer	<p>The Chief Privacy Officer (CPO) sets the strategic direction for Privacy within their agency. The CPO is responsible for:</p> <ul style="list-style-type: none"> • Dealing with any complaints from the Ministry staff or clients about possible privacy breaches • Dealing with requests for access to personal information, or correction of personal information • Acts as the liaison for the Ministry with the Office of the Privacy Commissioner • Advising the Ministry on the potential privacy impacts of changes to the organisation's business practices • Overseeing the function governing what the Ministry can and cannot do with personal information. <p>At the Ministry, the CPO is the GM Information.</p>
Information, Security and Identity Group	<p>The Information, Security and Identity Group is responsible for:</p> <ul style="list-style-type: none"> • Supporting MSD's strategic future – providing thought leadership on information security, privacy and information management across, as well as influencing information maturity growth across MSD and all of government • Delivering assurance - providing support to MSD in meeting its compliance responsibilities through an assurance programme to manage defined information risks. • Providing expert advice - providing specialist skills to ensure business processes and systems design align to good practice, including responsible use and protection of information assets and comply with information legislation and related regulations. • Delivering a foundational capability - providing direction, guidance tools, training and support for information capability improvements.
Strategy & Insights	<p>The Strategy & Insights Group is responsible for:</p> <ul style="list-style-type: none"> • Maintaining enterprise data resources, such as an enterprise data catalogue, enterprise data model, and their implementation into MSD's data warehouse, ensuring we can understand and

Person/Party	Responsibility
	<p>access our authoritative data sets with confidence in their quality, timeliness, and consistency.</p> <ul style="list-style-type: none"> • Driving MSD's approach to data and analytic products which support decision making, and ensuring we are recognising the potential value of a given use of data in trading off against risk. • Setting requirements for new data collection and standards around that data's quality and structure in order to be useful for analytics. • Supporting the Ministry to use and manage Ministry data, analytics, and evidence • Client and Business Intelligence and data science • Research and Evaluation to analyse data and produce insights that inform decision-making and provide evidence on what interventions work for whom • Data Management and data reporting.
Improvement, Systems and Technology (IST)	<p>IST is responsible for enabling people and partners with improved services and effective technology so New Zealanders can easily access the support they need.</p> <p>IST, as system owners, are responsible for the overall operation of the system, including any outsourced services, telecommunications, and cloud. IST is part of the Transformation Group and are made up of service improvement and technology experts, including Technology Security and Identity</p>
Ethics Advisor	<p>The Ethics Advisor is responsible for:</p> <ul style="list-style-type: none"> • Formulating, reviewing, and disseminating ethics-related documents, and providing guidance related to all ethical issues, including those relating to information (code of conduct, conflicts of interest, outside activities, etc.) <p>At MSD, the Ethics Advisor is an independent ethics advisor commissioned by the GM Information.</p>

Definitions

Word/ phrase	Definition
Algorithm	Algorithms are sets of instructions that enable computers to solve problems or complete tasks. There are many different types of algorithms for different purposes and outcomes. Algorithms can be simple or complex. All forms of 'AI' are complex algorithms.
Archiving	The process of preserving information that needs to be held over the medium or long term with low frequency of access, so that it retains its integrity and remains available for use by MSD and others until it is able to be disposed.
Information	Recorded information (including both personal information and data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email correspondence, datasets, audit logs, metadata (including reaction emoji 🐱), text messages, voice recording, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of information and data recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Lifecycle	The stages through which information passes, such as creation or collection, storage, access and sharing, use, maintenance and archiving, and disposal through destruction or transfer.
Information Governance	Enterprise Information Governance is a structured, consistent, and deliberate approach to managing, protecting, and using our information to support the Ministry's strategic objectives and fulfil mandated obligations. It unifies existing governance structures, clarifies decision-making processes, and identifies gaps across information-related capabilities. By embedding Te Ao Māori values and integrating the Information Accountability Framework and Information Policy Framework, it drives effective and accountable information management practices
Information Use	Information Use means everything that is done with information. This means not just active use, but also all parts of the information lifecycle (including collection and disposal). For the avoidance of doubt, information is being used when it is held in a database, even when that database is not actively being accessed.

Information Management	The process by which the Ministry ensures that information is managed across its lifecycle, such that it is accurate, relevant, and accessible; and that it is retained and disposed of appropriately in line with its value and its risk profile.
Information Security	Information Security relates to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".
Personal Information	Personal Information is defined under the Privacy Act 2020 as "Information about an identifiable individual...". It includes anything that relates to an identified person to be identified directly or indirectly, such as, but not limited to name, address, contact details, date of birth, signature, photographic image, Social Welfare Number, information about someone's health, sex life or orientation, their finances, religious, political or philosophical beliefs, race, biometric or genetic data.
Privacy	Privacy relates to the rights an individual has to control their personal information and how it's used. There is an obvious overlap between information security and privacy. This policy recognises the interdependence of one to the other.
Risk culture	The level of risk that an organisation is prepared to accept in pursuit of its objectives.

Privacy, Human Rights and Ethics Policy

Last Review Date:	November 2024
Next Review Date:	November 2026
Approved by:	Organisational Health Committee
Owner:	General Manager Information (CPO)

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) in upholding its Privacy, Human Rights and Ethics responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for how the Ministry respects people's privacy and human rights in an ethical manner through our use of information. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's information culture and decision-making.

Policy Statement

The Ministry holds and uses information about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

As the Ministry interacts with New Zealanders of different ages, backgrounds, ethnicities, genders and disabilities, consideration for people's privacy, human rights, ethics, bias, and discrimination must be at the centre of these interactions. This extends to how the Ministry partners and shares information with tangata whenua, communities, and other agencies, and commitment to adhering to the NZ Digital Government Data Protection and Use Policy (DPUP) principles. At all times the Ministry must uphold and maintain compliance with the Privacy Act 2020 and other relevant laws (such as the Human Rights Act 1993 and the Bill of Rights Act 1990).

Scope

This policy applies to all Ministry staff including contractors; all information held and used by the Ministry (physical and electronic); and all activity conducted by third parties on behalf of the Ministry.

Policy Principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry only collects the information it needs from people, and is transparent and clear about its purpose and use

Any information collected must be for a defined and intended purpose; limited to what is lawful, necessary and relevant to the Ministry's purpose and related activities. The Ministry collects this information in ways that are fair and not unreasonably intrusive.

Transparency is important for trust and respecting people's mana. When the Ministry collects information about people, it must tell them, in a way that makes sense to them, what information is collected about them, how it is used, and who it is shared with and why. This is done even if it is used or shared in a way that does not and cannot be used to identify them. Where this use involves algorithms making decisions about people, the Ministry also tell them about how the algorithms work, what role humans have in the decision-making process, and as relevant how any decisions can be challenged.

2. The Ministry uses information responsibly to support better decisions, better outcomes, and better lives

While delivering its services, the Ministry uses information to improve the client experience and help make better decisions for better lives and better outcomes. The information used must be protected as an extension of the whānau, people, and communities that it was collected from, and handled with dignity, care and respect.

3. The Ministry acts honestly, truthfully and with integrity when using and handling information

The Ministry recognises and, where possible, incorporates diverse cultural interests, backgrounds, perspectives, and needs when using and handling information. The Ministry is objective, fair, does not unjustifiably disadvantage others or discriminate (including through our use of algorithms or other tools).

4. The Ministry shares personal information responsibly

As public servants, the Ministry recognises that information is a powerful enabler for creating actionable intelligence, and leverages this taonga respectfully, ethically, and transparently. When sharing the personal information of clients and people, it is because the Ministry has a specific legal reason or their permission to do so. The Ministry is committed to sharing only what is needed to fulfil each purpose or request, including to help people get the support they need. The Ministry will work with other agencies to create and share value together from information collected, including by using de-identified data and analysis and by sharing research findings.

5. The Ministry empowers and enables people to access, correct and use their own information held by the Ministry

Where it is able, the Ministry supports the choices of clients and staff when making decisions about what personal information they want to share, how they want it used, and by whom. The Ministry encourages people to see what is collected and recorded about them and wherever possible give easy access to, and oversight and correction of, their information.

Roles and Responsibilities

Everyone that works for or is contracted to the Ministry has a responsibility to comply with this policy. The responsibility of each role specifically relevant to this policy is set out in the table below:

Person/Party	Responsibility
All Staff	<p>All staff (including contractors) are responsible for:</p> <ul style="list-style-type: none"> • Complying with the Ministry's information policies; • Following information guidance and training; • Identifying and reporting information security, information management, and privacy incidents; and • Escalating risks, as needed, to their manager.
Managers	<p>All managers are responsible for:</p> <ul style="list-style-type: none"> • Leading and facilitating regular information discussions with their teams; • Ensuring that their teams are familiar with the Ministry's information policies and guidance, use approved tools, and comply with the Ministry's information governance approach; • Providing direction on acceptable behaviours to their teams; • Modelling good information practice through their actions and behaviour; • Identifying and escalating information risks, as appropriate, to ensure they are managed effectively at the appropriate level and in a timely way; and • Reporting any IT security, information security or privacy incidents to their line manager.

Person/Party	Responsibility
Information Asset Owners	<p>All information assets owners are responsible for:</p> <ul style="list-style-type: none"> • Leading and championing a culture that values protection and responsible use of information; • Understanding which information assets they are accountable for, their value, where they come from, and how they are used; • Knowing who has access to that information and why and ensuring that access is controlled and reviewed continuously; • Ensuring that the risks to, and the opportunities for, their information assets are managed and monitored; and • Ensuring their information assets are fully utilised in line with responsible information use. <p>The information asset owner must understand the value of each information asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information involved.</p> <p>At the Ministry, Information Asset Owners will typically be assigned at the Tier 3 senior leader level, reporting directly to Deputy Chief Executives (DCEs).</p>
Information Stewards	<p>Information stewards are responsible for:</p> <ul style="list-style-type: none"> • Maintaining specialist knowledge about the information in their business area; • Ensuring information is available for its intended purpose; • Managing and maintaining information assets based on the Ministry's standards, policies, and other guardrails, including data quality, integrity and metadata; • Maintaining and updating an inventory of information assets; • Monitoring and optimising the lifecycle of information to manage risk and opportunities; • Collaborating with stakeholders across the business (including System Owners, other Information Stewards, Business Capability owners, and line 2

Person/Party	Responsibility
	<p>assurance functions) to implement the necessary guardrails;</p> <ul style="list-style-type: none"> • The responsible use of information assets, enabling the organisation and other agencies, where appropriate, to gain maximum value from the information; and • Supporting information asset owners to make informed decisions about the management and use of their asset for the duration of its lifecycle. <p>The Information Steward must keep the Information Asset Owner informed and made aware of any risks or concerns surrounding the integrity or safety of information.</p> <p>At the Ministry, Information Stewards will be assigned by the Information Asset Owners and are typically senior subject matter experts in their respective business areas.</p>
Information Governance Committees	<p>Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance. They set the overall risk culture for the Ministry which guides the way it responds to information risk and opportunity.</p> <p>These governance bodies must have membership from the Ministry's Leadership Team, as well as appropriate Māori representation, and have oversight of:</p> <ul style="list-style-type: none"> • Information and IT security policies and strategies; • Information standards and architecture; • Obligations contained in the Protective Security Requirements (PSR), the Privacy Maturity Assessment Framework (PMAF), and the Archives New Zealand Information and Records Management Standard; and • Ministry decisions about ensuring there are adequate systems, processes, and controls in place to identify and manage information risk. <p>At the Ministry, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC), and the Information and Protective Oversight Committee (IPSOC), the Transformation and Investment Committee, and Tai Nuku Design Committee.</p>
Executive Sponsor Information	<p>The Executive Sponsor champions the importance of information management among the organisation's leadership. The aim is for everyone in the organisation to see</p>

Person/Party	Responsibility
	<p>information management as an integral part of a business operating effectively. The Executive Sponsor Information is responsible for:</p> <ul style="list-style-type: none"> • Ensuring the strategy and policy adopted by the organisation supports information management; • Being involved in strategic and operational planning to align information management with the corporate objectives and business activities of the organisation; • Liaising with business units to ensure information is integrated into work processes, systems, and services; • Overseeing the budget for information and ensuring the resources needed to support information are known and sought in funding decisions; • Ensuring staff with appropriate skills to implement information strategies are employed, and regular upskilling is available; and • Monitoring and reviewing information to ensure it is implemented, transparent and meets business needs. <p>The CE has delegated the Executive Sponsor Information role to the DCE Organisational Assurance and Communication (OAC).</p>
Chief Privacy Officer	<p>The Chief Privacy Officer (CPO) sets the strategic direction for Privacy within their agency. The CPO is responsible for:</p> <ul style="list-style-type: none"> • Dealing with any complaints from Ministry staff or clients about possible privacy breaches and setting parameters for how they are managed; • Dealing with requests for access to personal information, or correction of personal information; • Acting as the liaison for the Ministry with the Office of the Privacy Commissioner; • Advising the Ministry on the potential privacy impacts of changes to the organisation's business practices; and • Overseeing the function governing what the Ministry can and cannot do with personal information. <p>At the Ministry, the Chief Privacy Officer (CPO) is the General Manager Information. The CPO is responsible for implementing and having assurance over this policy.</p>

Person/Party	Responsibility
Information, Security and Identity Group	<p>The Information, Security and Identity Group is responsible for:</p> <ul style="list-style-type: none"> • Supporting the Ministry's strategic future – providing thought leadership on information security, privacy and information management, as well as influencing information maturity growth across MSD and all of government; • Delivering assurance - providing support to the Ministry in meeting its compliance responsibilities through an assurance programme to manage defined information risks; • Providing expert advice - providing specialist skills to ensure business processes and systems design align to good practice and comply with information legislation and related regulations; and • Delivering a foundational capability - providing direction, guidance tools, training and support for information capability improvements.
Strategy and Insights	<p>The Strategy and Insights Group is responsible for:</p> <ul style="list-style-type: none"> • Maintaining enterprise data resources, such as an enterprise data catalogue, enterprise data model, and their implementation into the Ministry's data warehouse, ensuring we can understand and access our authoritative data sets with confidence in their quality, timeliness, and consistency; • Driving the Ministry's approach to data and analytic products which support decision making, and ensuring we are recognising the potential value of a given use of data in trading off against risk; • Setting requirements for new data collection and standards around that data's quality and structure in order to be useful for analytics; • Supporting the Ministry to use and manage Ministry data, analytics, and evidence; • Client and Business Intelligence and data science; • Research and Evaluation to analyse data and produce insights that inform decision-making and provide evidence on what interventions work for whom; and • Data Management and data reporting.

Person/Party	Responsibility
Improvement, Systems and Technology (IST)	<p>IST is responsible for:</p> <ul style="list-style-type: none"> Enabling people and partners with improved services and effective technology so New Zealanders can easily access the support they need; and The overall operation of the system, including any outsourced services, telecommunications, and cloud. <p>IST is part of the Transformation Group and are made up of service improvement and technology experts.</p>
Ethics Advisor	<p>The Ethics Advisor is responsible for:</p> <ul style="list-style-type: none"> Formulating, reviewing, and disseminating ethics related documents, and providing guidance related to all ethical issues relating to information. <p>At the Ministry, the Ethics Advisor is an independent ethics advisor commissioned by the GM Information.</p>

Definitions

Word/ phrase	Definition
Bias	The action of supporting or opposing a particular person, group or thing in an unfair way compared to other people or things.
Discrimination	The act of making distinctions between people based on the groups, classes, or other categories to which they belong or are perceived to belong. People may be discriminated on the basis of race, gender, age, religion, disability, or sexual orientation, as well as other categories.
Ethics	Well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues.
Human Rights	The recognition of the inherent value of each person, regardless of background, where they live, what they look like, what they think or what they believe. Human Rights are based on principles of dignity, equality, and mutual respect.
Algorithm	<p>Algorithms are a sets of instructions that enable computers to solve problems or complete tasks.</p> <p>There are many different types of algorithms for different purposes and outcomes.</p>

	Algorithms can be simple or complex. All forms of 'AI' are complex algorithms.
Information	Recorded information (including both personal information and data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email correspondence, datasets, audit logs, metadata (including reaction emojis 🐱), text messages, voice recording, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of information and data recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Sharing	The exchanging, collecting, sharing, or disclosing of personal information by secure means to other parties within the Ministry, or with other organisations, for certain purposes.
Information Use	Information Use means everything that is done with information. This means not just active use, but also all parts of the information lifecycle (including collection and disposal). For the avoidance of doubt, information is being used when it is held in a database, even when that database is not actively being accessed.
Personal Information	Personal Information is defined under the Privacy Act 2020 as "Information about an identifiable individual...". It includes anything that relates to an identified person to be identified directly or indirectly, such as, but not limited to name, address, contact details, date of birth, signature, photographic image, Social Welfare Number, information about someone's health, sex life or orientation, their finances, religious, political or philosophical beliefs, race, biometric or genetic data.
Privacy	Privacy relates to the rights an individual has to control their personal information and how it's used. There is an overlap between information security and privacy. This policy recognises the interdependence of one to the other.