



27 February 2025

Tēnā koe

Official Information Act Request

Thank you for your email of 29 January 2025, requesting information about the Ministry's privacy compliance program.

I have considered your request under the Official Information Act 1982 (the Act). Please find my decision on each part of your request set out separately below. Please note that the documents attached and listed below may fall in scope of multiple sections of this request.

1. Privacy standards and frameworks

Please refer to the following four documents attached:

- 01. Automated Decision-Making Standard.
- 02. Recording Standard.
- 03. Client Identity Verification Standard.
- 04. Survey Standard.

2. Employee privacy policy

Please refer to the following document attached:

- 14. Personal Employment Information Policy.

3. Privacy audit templates and related tools

Please refer to the following document attached:

- 05. Scene Setting – Privacy.

The Ministry conducts a yearly privacy maturity assessment, this framework and self-assessment form is public and can be found through the following link:
www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/self-assessment-forms

The Ministry also undertakes audits on its Approved Information Sharing Agreements (AISA) as necessary however there is no standard template for these assessments. More information on these AISA's can be found here:
www.privacy.org.nz/privacy-act-2020/information-sharing/approved-information-sharing-agreements

4. Privacy Impact Assessment (PIA) templates and guidelines

Please refer to the following document attached:

- 06. Security, Privacy, Human Rights and Ethics Assessment Template (please note that this document is in scope of question 3 above also).

5. Privacy breach reporting templates, including assessments and post-incident review templates

Please refer to the following two documents attached:

- 07. Forms- Privacy or IT Security Incident Form.
- 08. Risk matrix for privacy breach details.

6. Access and correction request response templates and standards

Please refer to the following document attached:

- 09. Privacy Act Request Templates.

The Ministry does not have standard templates for the correction of information however more information on how clients are able to correct their personal information can be found here: www.workandincome.govt.nz/about-work-and-income/privacy-notice/managing-your-information.html

7. Standard legal clauses for privacy in commercial contracts

Please refer to the following document attached:

- 10. Commercial Contract Privacy Clauses.

8. Documentation on how the organisation ensures compliance with privacy legislation and regulation.

9. Any other relevant templates, policies, or frameworks used by the organisation to manage privacy and data protection obligations

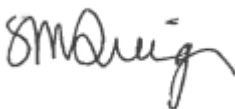
Please refer to the following three documents:

- 11. Information Governance Policy.
- 12. Privacy Human Rights and Ethics Framework.
- 13. Template Information Sharing Memorandum of Understanding.

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, 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

Automated Decision Making Standard

Approved by:	Leadership Team
Standard Owner:	General Manager Information
Review date:	1 March 2025

1 Definitions

- 1.1. **Automation** is the use of systems or components of systems to replace repeatable processes in order to reduce dependency on manual actions or interventions.
- 1.2. Processes can be automated based on the application of:
 - (i) known business rules, and/or
 - (ii) data-based algorithms without involvement or assessment by a human, including statistically or analytically derived patterns in machine learning or Artificial Intelligence.
- 1.3. A **decision** for the purpose of this standard is the action of choosing between two or more possible actions and may be derived from legislative, cabinet or other legal authority or can be operational, and may be discretionary or non-discretionary.
- 1.4. An **automated decision** for the purpose of this standard is a decision within an automated process where there is no substantial human involvement in making the decision.
- 1.5. **Discretionary decisions** require an exercise of judgment to choose between two or more possible actions.
- 1.6. A non-discretionary decision **does not** require any exercise of judgement to determine the appropriate action.
- 1.7. A **Business Owner** is the person who is accountable for the automated process at any given time.
- 1.8. For the purposes of this standard, "**bias**" refers to the tendency of an automated decision process to create unfair and unjustified outcomes, such as favouring or disfavouring one group over others.
- 1.9. Automated decisions may be biased because, for instance, the **datasets** they rely on are biased, potentially as a result of how data was collected in the past, or because **social conditions** mean that some groups are overrepresented in some risk groups.
- 1.10. The prohibited grounds of discrimination are set out in the **Human Rights Act 1993 Section 21**: sex, marital status, religious belief, ethical belief, colour, race, ethnic or national origins, disability, age, political opinion, employment status, family status and sexual orientation.
- 1.11. Discrimination on these grounds can be justified under the **Bill of Rights Act 1990 Section 5**, but only to such reasonable limits that are lawful and can be clearly and ethically justified.

2 Applicability

- 2.1 This standard **must** be applied using the operational guidance when:
- (i) there is a proposal to automate a decision (as defined in sections 1.3 and 1.4), **AND**
 - (ii) the automated decision has the **potential to affect**, an individual's entitlement, obligations, or eligibility status for support delivered or funded by the Ministry of Social Development (the Ministry).
- 2.2 Where a complex algorithm is being proposed, the Model Development Lifecycle **must** be used.
- 2.3 Any exception to this standard **must** be approved by the Chief Executive before automated decision-making can be implemented.

3 Standard Requirements

3.1 General

- 3.1.1 Automated decision-making **must**:
- (i) improve efficiencies and effectiveness of decision making and balance factors such as cost, accuracy, reliability and safeguarding the wellbeing of those affected.
 - (ii) comply with all applicable Ministry policies and standards that relate to the privacy, security and management of information.
- 3.1.2 Automated decision-making **must not** create inefficiencies for those the decisions directly affect, for example, creating manual workarounds for a client to enable automation, or unnecessarily increasing time from application to notification of a decision than would otherwise occur if it was manually completed.
- 3.1.3 There **must** be clear, relevant, and accessible guidance for users who are required to input or provide data to be used in automated decision-making, for example, a service user entering their information in MyMSD.

3.2 Accuracy, bias and discrimination

- 3.2.1 Accuracy and reliability **must** be assessed before automated decision-making is implemented to ensure, insofar as possible, that automated decision-making is producing expected results, that automated decisions do not deny clients full and correct entitlement (FACE), and bias and discrimination is well managed.
- 3.2.2 Based on the assessment carried out under 3.2.1, where evidence suggests that automated decision-making has resulted in unintended bias, steps **must** be taken to identify and remove or mitigate the unintended bias, and any residual risk **must** be accepted by the Business Owner.
- 3.2.3 Where unintended bias cannot be removed or sufficiently mitigated, substantial human involvement **must** be included in the process. This would then mean that the decision is no longer an automated decision.

3.3 Policy, fraud and legal considerations

- 3.3.1 Automated decisions **must** be lawful and align with policy intent.

3.3.2 An assessment must be undertaken to determine whether any proposed automated decision-making has the potential to:

- (i) increase (or decrease) the likelihood that people will commit internal or external fraud or client non-compliance; or
- (ii) Increase (or decrease) the scale or size of potential internal or external fraud or client non-compliance.

3.3.4 Prior to automating discretionary decisions, you **must** ensure that any legal risk(s) are identified and mitigated or accepted by the Business Owner before automated decision-making can be implemented.

3.4.1 The Ministry **must** make information publicly available about:

- (i) what policies and processes are used to identify and mitigate risks associated with automated decision-making, in particular those that relate to human rights and ethics; and
- (ii) what decisions are made using automated decision-making as soon as reasonably practicable after they have been:
 - a. identified;
 - b. assessed against the Standard; and
 - c. approved by the Business Owner and the Standard Owner.

3.4.2 The Ministry **must** provide as much transparency as possible, while minimising the risk of fraud, to clearly explain how a decision has been made through the use of automation, including the role of humans in automating the decision and who is accountable for the process and the decision made.

3.4.3 If a lawful restriction prevents explanation, the Ministry **must** provide as much explanation as possible to the individual and clearly outline what details have been withheld and why.

3.4.4 The use of automated decision-making **must** be communicated to the individual in a way that is easy to understand and clearly shows a decision was made using automation, the outcome of that decision, and the process for challenging or appealing decisions.

3.5.1 A visible and accessible point of contact **must** be nominated for public inquiries about decisions made using automation.

3.5.2 The Ministry **must** provide a channel for challenging or appealing decisions made using automation and this channel **must** be made easily visible and accessible to the individual(s) impacted by the decision.

3.5.3 The process to review an automated decision that has been challenged or appealed **must not** itself be an automated process.

3.6 Compliance and assurance

- 3.6.1 Compliance with this standard **must** be verified for all new uses of automated decision-making through the existing Security, Privacy, Human Rights and Ethics Certification and Accreditation process.
- 3.6.2 Regular monitoring **must** be carried out to ensure that the automated decision-making continues to produce expected results and to ensure bias and discrimination are well managed.
- 3.6.3 A compliance review **must** be carried out at least once every three years or more frequently (based on the nature and level of risk connected to the process) to ensure that any automated decision-making that is approved under this standard continues to meet the requirements of the standard.

4 References

- 4.1.1 Principal tools and policies used as inputs in the development of this Standard.

[Principles for Safe and Effective Use of Data and Analytics](#)

[Algorithm Charter for Aotearoa New Zealand](#)

[Data Protection and Use Policy](#)

- 4.1.2 Tools that directly support the application of this Standard.

[Operational Guidance](#)

[Data Model Lifecycle](#)

[PHRaE guidance: Operational analytics and automation](#)

Recording Standard

Approved by: Privacy & Security Oversight Board (PSOB) on 13 April 2022

Next Review Date: April 2024

Owner: General Manager Information

1 Overview

1.1 Purpose

- 1.1.1 This standard sets out the minimum requirements to ensure that MSD meets its obligations under the Privacy Act 2020 (Privacy Act) when making recordings for operational purposes.

1.2 Definitions

- 1.2.1 **Recording** refers to speech or moving pictures that have been captured to be listened to or watched later. It does not refer to the process or business of storing them.
- 1.2.2 **Meeting** is an occasion when people come together, either in person or online, to discuss something, and can include announcements.
- 1.2.3 **Internal Event or event** means a meeting that is only attended by MSD personnel.
- 1.2.4 **Client meeting** is any meeting or discussion with an MSD client regardless of whether this interaction is face to face, phone based or via other methods.
- 1.2.5 **External event** is any meeting, community gathering, function, or a public event that is attended by non-MSD personnel and is hosted or attended by MSD personnel.

1.3 Scope

- 1.3.1 This standard **must** be applied, using the operational guidance, when recording:
- (i) Any images through **CCTV**
 - (ii) Inbound and outbound calls at the **Contact Centre**
 - (iii) Any **external events** MSD hosts, attends, or for internal or external public relations purposes.
 - (iv) An **internal event**
 - (v) A **client meeting**
- 1.3.2 This standard **must** be applied by all staff, third parties and contractors who record, or handle recorded information, on behalf of MSD.
- 1.3.3 This standard **must** be applied equally to formal interviews as well as less formal conversations and other interactions that are recorded.
- 1.3.4 MSD must grant reasonable requests from non-MSD personnel to record their interactions with MSD.

2 Standard

2.1 General

- 2.1.1 There **must** be a clear purpose and justification for recording the meeting.
- 2.1.2 All parties **must** be able to understand why the recording is happening.
- 2.1.3 Any reasonable objection or instruction from an attendee **must** be considered, such as a request:
 - (i) Not to capture their image
 - (ii) Not to capture their voice
 - (iii) To note their objection or instruction.
- 2.1.4 If a reasonable objection or situation is present that prevents recording, a formal record of the events **must** be made via other means i.e., minutes etc.

2.2 Access and retention

- 2.2.1 Any recording **must** be stored in line with the [guidance](#) for managing Ministry information.
- 2.2.2 Any party to a recording **must** be able to request access to a copy of this, as it is classed as personal information we hold about them.
- 2.2.3 Any recording **must** only be retained for as long as it is required in line with the original, or a directly related, purpose.

2.3 Use

- 2.3.1 A recording **must not** be used for a purpose different to, or not directly connected to, the original reason for making the recording.

2.4 Technology and equipment

- 2.4.1 For recording being facilitated by MSD, only tools approved for recording **must** be used.
- 2.4.2 If you feel there isn't a [tool](#) that meets your needs or would like to check, you **must** contact the Information Management team at infohelp@msd.govt.nz.

2.5 Transparency and notification

- 2.5.1 The fact a meeting is being recorded, its purpose and the intended use of the recording **must** be understood by all potential and actual attendees and captured as part of the recording.
- 2.5.2 All those that may be captured in any recording **must** be given reasonable opportunity to consent.
- 2.5.3 If recording cannot take place without capturing others not party to the meeting or who have not given their consent, then the recording **must not** be created and an alternative method of capturing the information should be used.
- 2.5.4 If it becomes apparent after a recording has taken place that someone was unexpectedly included in the recording all reasonable steps **must** be taken to resolve the situation in accordance with the process set out in the operational guidance.

- 2.5.5 Participants **must** be given reasonable opportunity to access or review the accuracy of any minutes or transcription created from a recording, if requested.

3 Standard Compliance

3.1 Exceptions

- 3.1.1 Any exception to this Standard **must** be approved by the General Manager Information in advance.

3.2 Compliance Measurement

- 3.2.1 A review **must** be carried out at least once every three years or more frequently (based on the nature and level of risk connected to the process) to ensure that any recording made of handled meets the actions required under this standard.
- 3.2.2 Compliance to this standard will be measured through the assessment of retention and deletion activities, use of, and fulfilment of any related Privacy Act requests for personal information connected to recordings.

4 References

Privacy Act

Operational Guidance (in development)

Data Protection and Use Policy

Information Hub (containing information policies, standards and guidelines)

Client Identity Verification Standard

Approved by:	GM Information on 20/09/2023
Standard Owner:	GM Information
Next Review Date:	September - 2025
Review Committee	Information Policies & Standards Working Group (IPSWG)

1 Purpose

This standard describes the Ministry of Social Development (the Ministry) expectations and requirements for verifying a client's identity. Aligning your identity verification process and/or guidelines with this standard will enable the Ministry to have a known level of trust and confidence that clients are genuinely who they claim to be.

This standard can also be shared with third-party vendors to set the Ministry's expectation for identity verification processes. It is expected that third parties must meet the requirements stated in this standard and provide evidence (e.g., signed policy, patch report).

2 Scope

This standard covers the minimum identity verification requirements for all Ministry systems, network assets, and computing devices used to conduct Ministry business or interact with internal/external networks and business systems, whether owned by the Ministry, the employee, or a third party. This includes systems that contain company or customer data owned or managed by the Ministry, regardless of location.

This standard applies to employees, contractors, consultants, temporaries, and other workers at the Ministry of Social Development, including all personnel affiliated with third parties.

Definitions can be found at the bottom of this standard.

3 Standard

3.1 DIA reference standards and definitions

The framework and process for constructing this standard has been supplied by the Department of Internal Affairs (DIA). Core content and definitions have come from all-of-Government definitions set out in the DIA Identity Management Standards¹ and



¹ Source: *DIA Identification Management Standards* (link: <https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/>)

these are explicitly referenced throughout this document and included in **Section 6** of the standard.

A critical component of the DIA reference standards is that it utilises an assurance-based risk model. This involves setting requirements for identity verification in an organisation based on the levels of risk inherent in the delivery of its products and services. The level of risk identified then translates directly to a 'level of assurance' (LOA) required to best manage the identified risk.

The requirements within this document are based on a 'level of assurance three' (LOA3) from the DIA Identification Management Standards, supplemented with a set of custom requirements for MSD based on the scope above and in following the process outlined by DIA. This level of assurance was selected after a risk assessment was completed with a working group of diverse representation to ensure broad coverage of MSD's products, services, and interests².

3.2 Client identity verification objectives

Confirming a client's identity (a set of information that represents a person), will involve fulfilling four (4) objectives:

- 3.2.1 Establish that an identity is unique.
- 3.2.2 Establish that an identity has not been fraudulently created.
- 3.2.3 Establish the use of an identity (through interactions with Government and the community) over time.
- 3.2.4 Establish confidence in the linkage between an identity and the person who is claiming the identity.

3.3 Principles of assurance

- 3.3.1 MSD will use levels of assurance to determine its confidence level in a client's identity.
- 3.3.2 The level of assurance required (LOA3) (**Section 6**) will be achieved for each client to receive a product or service for the first time to achieve a high confidence in the claimed or asserted identity.
- 3.3.3 Assurance is achieved through ensuring MSD has the right information about the right client.

3.4 Requirements

Requirement key

Requirement Type	Interpretation
MUST	An absolute requirement.
SHOULD	Defines a recommended course of action that may be ignored if the full implications of doing so are clearly understood and MSD is prepared to accept them.

² Source: *MSD R&A client verification risk assessment_endorsed 29Oct20* (link: <https://objective.ssi.govt.nz/documents/A13076295/>)

Information is protected

Identity information is protected, and measures are in place to prevent identity theft by building protections into the collection and storage of information:

- 3.4.1 MSD **MUST** have a justifiable need for every piece of information it collects.
- 3.4.2 MSD **MUST** store only the information it requires to carry out its purpose.
- 3.4.3 Where information is collected for the sole purpose of verifying an identity, once the identity is confirmed, MSD **MUST** discard this information.
- 3.4.4 Where identity verification processes include facilitated events, MSD **MUST** keep a record that the information was collected, and the verification process undertaken.
- 3.4.5 MSD **MUST** collect enough distinctive information when it verifies client's identity to ensure one client can be distinguishable from another client.

Information is accurate

Identity information is accurate, and measures are in place to determine the quality of the information being used to verify a client's identity:

- 3.4.6 MSD **MUST** seek assurance that the information provided on an identity credential (e.g. NZ Passport) is accurate.
- 3.4.7 Information provided on an identity credential used to verify a client's identity **MUST** be from an authoritative source (i.e. cannot have been altered since it was delivered from this source) or a certified copy (**Section 6**).
 - Where an original document cannot be sourced, MSD **MUST** accept certified copies of identity documents (this is an MSD specific standard).
 - In accepting certified copies, MSD **SHOULD** be satisfied that the documents provided are true copies.

Quality of identity information

- 3.4.8 MSD **MUST** assess the quality of a credential; this can be completed digitally or manually (e.g., NZ Drivers Licence) and/or by assessing physical security features (e.g., holographic text on a NZ Drivers Licence) of a credential where they exist.
- 3.4.9 MSD **MUST** ensure the integrity of a facilitated identity verification events by assessing the security features (e.g., verifiable Credential Provider identifiers, digital certificates, asynchronous keys, encryption, authentication channels and cryptographically signing the verification event).
- 3.4.10 MSD **SHOULD** ensure an identity credential has not been revoked by the credential provider.
- 3.4.11 MSD **MUST** check the expiration and issue dates for documents used as evidence of identity:
 - 'Category A' (**Appendix 1**) documents **MUST** be current or have expired no more than 2 years ago.
 - 'Category B' (**Appendix 2**) documents **MUST** be current.
 - 'Category B' (**Appendix 2**) documents marked with an (*) **MUST** be issued within the last six months.

- 3.4.12 Facilitated identity verification events generated based on documents that do not meet the expiry and issue dates as specified under 3.4.11 **MUST** only be accepted where the risk to MSD has been assessed and where this risk has been accepted by the GM Integrity and Debt prior to the solution being implemented. This assessment is per solution, not per event.

Identifying client information

Client information must be specific to a single client and have a legitimate association.

- 3.4.13 MSD **MUST** ensure a client provides enough information to identify a distinct client record.
- 3.4.14 MSD **MUST** be able to identify when an identity has been claimed.

Linking the Client to their information

A client must be the subject of the client information (or credential) they have provided:

- 3.4.15 MSD **MUST** bind³ a client to their information in a way that establishes a relationship between the client and the identity information collected.
- 3.4.16 MSD **MUST** select binding methods using the following 'binding factor' types:
- 3.4.16.1 possession factors (e.g., In possession of a credential) that contain enough features to assess as genuine
 - 3.4.16.2 biometric factors (e.g., Photo on a credential) with appropriate measures to detect spoofing attempts (e.g., recordings, masks, make-up, or prosthetics etc.)
 - 3.4.16.3 knowledge factors that are not publicly known, easily determined, or predictable.
- 3.4.17 MSD **MUST** use a minimum of two (2) binding factor types.
- 3.4.18 MSD **MUST** limit the number of unsuccessful attempts to bind, disallow further attempts, and trigger further investigation in the circumstance of excessive unsuccessful attempts to bind.
- 3.4.19 MSD **MUST** ensure clients have in their possession and control when completing the verification process (**Appendix 3**):
- a New Zealand Passport, or
 - a New Zealand Driver Licence, or
 - Two (2) 'Category A' documents (**Appendix 1**) where one (1) 'Category A' document must have a photo, or
 - One (1) 'Category A' document (**Appendix 1**) and one (1) 'Category B' document (**Appendix 2**), where the 'Category A' document must have a photo.
- 3.4.20 If the documents provided by a client or used for identity verification have different names but are current and valid. An acceptable change of name document **MUST** be provided (**Appendix 4**).

³ The process of linking a person to a piece of information.

Client cannot be linked to information due to insufficient documentation

3.4.21 For clients unable to provide the required identity documentation, all efforts **SHOULD** be made to obtain satisfactory identity verification either before payment is approved or within 12 weeks of payment.

- MSD **SHOULD** make an ongoing effort to establish a confirmed identity.
- To meet the standard, there is an identity referee process (**Appendix 5**) as well as supporting documents that can be provided from Category B (**Appendix 2**).

Client information is distinguishable

Client information needs to be unique and distinguishable from another client's information:

3.4.22 MSD **MUST** ensure a client cannot claim more than one instance of client information (i.e. a client shouldn't be able to claim multiple identities).

- If a client fails to meet the MSD identity verification processes, a record **MUST** be created that contains the reasons for this outcome.
- If a client fails to successfully complete a facilitated identity verification process a record **MUST** be created that contains the reasons for this outcome.

Retest client binding

The link between a client and their information needs to be maintained as it can change over time:

3.4.23 MSD **MUST** retest the binding of a client to their identity information at least once every 5 years or on application for financial services and products. Note: each time a client engages with MSD and verifies their identity, this qualifies as a retest.

Binding timeliness

The client is bound to information on a credential and bound to a biometric (e.g., a photo) within one hour after the completion of an identity verification event:

3.4.24 MSD **MUST** ensure that binding and the checking of client information to an authoritative source is done in the same transaction or session.

Facilitated Identity Verification Events

3.4.25 MSD **MUST** ensure the client provides consent to have their identity information shared with MSD before accepting a facilitated identity verification event for that client.

3.4.26 MSD **MUST** only accept identity verification events facilitated by third parties that are at minimum Level of Assurance 3.

3.4.27 MSD **MUST** ensure that identity verification events facilitated by third parties provide at least:

- Transaction identifier: A unique identifier for the presentation
- Issuance: A timestamp indicating when the Credential was established (updated)

- Expiration: A timestamp indicating when the Credential is expected to expire
- Credential validity: Information and/or mechanisms for determining the validity of the Credential

4 Standard Compliance

4.1 Exceptions

If one or more requirements from this standard cannot be met, the system owner or manager must apply for an exception to the standard.

Applications for an exception to this standard must be sent to the GM Information. Please provide the following information in the email:

- A brief description of the system or service that is non-compliant
- Which standard requirement(s) cannot be met?
- Why are you failing to meet the requirement(s)?
- When can you estimate the system or service will be fully compliant?

4.2 Compliance Measurement

The GM Information will verify compliance to this standard through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the policy owner.

4.3 Non-compliance

Any employee found to have violated this standard **MAY** be subject to disciplinary action as per the Ministry's Human Resources (HR) manual. This could include formal reprimands up to and including termination of employment

5 Revision History

Date of Change	Responsible	Summary of Change
September 2023	Ross Drury	Change to include facilitated identity events and move to new standards template.
July 2021	Ellery hart	Update to 1.2
November 2020	Judy Brown	Initial Version

6 Definitions

Word / Phrase	Definition
---------------	------------

Agent	<p>An agent is a person or organisation who acts in the interests of another. A person can be made an agent by the consent of both the client and the prospective agent, by way of a Court Order or, in exceptional circumstances, without a client's consent.</p> <p>'Agency' refers to the relationship that arises where one person is appointed to act as the representative of another.</p>
Authenticate	Ensuring the same person is returning to access a system or service
authentication	Means a formalised process of verification, that, if successful results in an authenticated client.
authenticated identity	Means identity information for a client, created to record the result of authentication
authentication assurance	Means robustness of the process to ensure an Authenticator remains solely in control of its holder
authoritative source	<p>An authoritative source is a single, distinct, absolute original version of a document that is unique, identifiable and unalterable without detection. It cannot have been altered since it was delivered from the authoritative source eg. a passport.</p>
beneficiary	<p>Means a person who is:</p> <ul style="list-style-type: none"> (i) a person who has been granted a benefit; or (ii) a person in respect of whom a benefit, or part of a benefit, has been granted.
binding	<p>Refers to the process of securely associating or linking an entity (like a client or a user) with their identity information (like a credential) or an authenticator (like a biometric factor).</p> <p><i>Binding is about creating a strong and reliable association between a person or entity and the information or authentication methods used to verify their identity. It's the process that ensures the person presenting the identity information or using the authenticator is indeed the person they claim to be.</i></p>
binding assurance	Means the robustness of the process to bind the Entity-to-Entity Information and/or Entity to Authenticator.
Certified Copy	<p>A duplicate of an original document that has been verified as a true and accurate reproduction of the original. This verification is typically performed by a trusted, authoritative figure, such as a Justice of the Peace, a solicitor, or another authorised person, depending on the jurisdiction.</p> <p><i>In the process of certification, the authorised person will compare the copy to the original document to ensure that all information is correctly duplicated, and then they will attach a signed statement (or stamp) to the copy, declaring that they have confirmed its accuracy. This certification process provides assurance that the document has not been altered in any way and accurately represents the original.</i></p>

client	Means a person of which identity information is stored and managed for an identity management system and by MSD
credential	Means the representation of an identity for use in verification or authentication
Facilitated Verification Event	A facilitated verification event in the context of identity management refers to a process where a third party helps validate or confirm a person's identity. This is often utilised when there's a need to establish or confirm a person's identity without the person being physically present or available to the requester.
factors	Means: <ul style="list-style-type: none"> ➤ something the Client knows (knowledge factor) ➤ something the Client has (possession factor) ➤ something the Client is or does (biometric factor).
identifier	Means attribute or set of attributes that uniquely characterises an identity
identification	Means a process of recognising a Client in a particular domain as distinct from other clients
identity information authority [authenticated source]	A party that can make provable statements on the validity and or correctness of one or more attribute values in an identity
identity information provider	Means a party that makes client available identity information, this includes approved verification service providers
identity information check	Means a check that is carried out for the purpose described in the IICA Act
information assurance	Means robustness of the process to establish the quality and accuracy of Client Information
LOA (Level of Assurance)	Levels of Assurance: <p>LOA1 (Low) Little or no confidence in the claimed or asserted identity</p> <p>LOA2 (Medium) Some confidence in the claimed or asserted identity</p> <p>LOA3 (High) High confidence in the claimed or asserted identity</p> <p>LOA4 (Very High) Very high confidence in the claimed or asserted identity</p>
MSD	Ministry of Social Development
partner	In the phrase "spouse or partner" and in related contexts, means a civil union partner or de facto partner

unique identifier	Means an identifier other than the individual's name that uniquely identifies the individual
verification	Means a process of establishing the identity information (or credential) associated with a client
verifier	Means a party that performs verification

Appendix 1: Category A documents

This appendix contains supplementary/ standalone information to support the operationalisation of this standard and is intended to be updated in line with changes to MSD's processes through time.

Current document	Details	Issued by
NZ Passport	Issued in Client name	Department of Internal Affairs (DIA)
NZ Driver Licence	Issued in Client name This includes current learner permits and provisional licences.	Waka Kotahi – NZ Transport Agency
Overseas Passport	Issued in Client name	Overseas Authority
Australian Driver Licence	Issued in Client name This includes current learner permits and provisional licences.	Australian State Government Licensing Authority
NZ Emergency Travel Document	Issued in Client name	Department of Internal Affairs (DIA)
NZ Refugee Travel Document	Issued in Client name	Department of Internal Affairs (DIA)
NZ Certificate of Identity (issued under the Passports Act 1992)	Issued in Client name	Department of Internal Affairs (DIA)
NZ Certificate of Identity (issued under the Immigration Act 2009)	Issued in Client name	Ministry of Business, Innovation, and Employment (MBIE)
NZ Firearms Licence	Issued in Client name	NZ Police
NZ Birth Certificate (Issued on or after 1 January 1998, which carries a unique identifier)	Issued in Client name	Department of Internal Affairs (DIA)

Appendix 2: Category B supporting documents

This appendix contains supplementary/ standalone information to support the operationalisation of this standard and is intended to be updated in line with changes to MSD's processes through time.

Current document	Issued by
Kiwi Access Card (formerly known as the 18+ card)	Hospitality Association of NZ
Community Services Card	MSD
Super Gold Card	MSD
Veteran Super Gold Card	MSD
NZ Student Photo ID Card	NZ Educational Institution
NZ Employee Photo ID Card	Employer
NZ Electoral Role Record	Enrolment Centre of NZ Post
Inland Revenue Number Government document or correspondence containing suitable identity information	IRD Government departments
* NZ issued Utility Bill or Bank Statement	Utility Provider or Bank
Overseas Driver Licence	Overseas Authority
Steps to Freedom Form	Department of Corrections
* Household Accounts (tenancy agreement, documents from suppliers of goods and services such as hire purchase agreements)	Tenancy Services, goods/services provider
* Employment related documents (letter from employer or payslips)	Employer
* Bank/insurance company documents	Mortgage papers or insurance policies
* Health/education documents	Student identification card, school report, school leaving certificate, doctors bill, degree or trade certificate
* Prominent community member support letter	Support letters from people such as: New Zealand Police, Justice of the Peace, doctor, kaumatua, clergyman or Women's Refuge coordinator. Note: the person providing the reference must not live at the same address, not be related to the client and must have known the client for over 12 months.

Appendix 3: Documents clients must have in their possession and control when completing the verification process

A client must have in their possession and control when completing the verification process, documentation from one of the four below options

A New Zealand Passport



B New Zealand Driver's Licence



C 2 of the following, where one must have a photo



- Australian Driver Licence
- NZ Emergency Travel Document
- NZ Refugee Travel Document
- NZ Certificate of Identity (issued under the Passports Act 1992)
- NZ Certificate of Identity (issued under the Immigration Act 2009)
- NZ Firearms Licence
- NZ Birth Certificate (Issued on or after 1 January 1998, which carries a unique identifier)

D 1 of the documents from option C, where one must have a photo



AND

1 of the following

- Kiwi Access Card
- Community Services Card
- Super Gold Card
- Veteran Super Gold Card
- NZ Student Photo ID Card
- NZ Employee Photo ID Card
- NZ Electoral Role Record
- IR Number Govt document or correspondence containing suitable identity information
- NZ issued utility bill or bank statement
- Overseas Driver Licence
- Steps to Freedom form
- Household accounts
- Employment related documents
- Bank/insurance company documents
- Health/education documents
- Prominent community member support letter

Appendix 4: Name change documents

This appendix contains supplementary/ standalone information to support the operationalisation of this standard and is intended to be updated in line with changes to MSD's processes through time.

Current document	Details	Issued by
NZ Birth Certificate/s and name change document	Showing both names	DIA (Identity Service)
Marriage or civil union certificate	Showing both names	DIA (Identity Service)
Dissolution of marriage or civil union order	Showing both names	Ministry of Justice
Certificate of annulment	Showing both names	Ministry of Justice
Deed Poll certificate, change of name certificate	Showing both names	DIA (Identity Service)
Statutory declaration confirming change of name has been registered with the Registrar of Births, Deaths and Marriages	Showing both names	DIA (Identity Service)

Appendix 5: Authorised identity referees

This appendix contains supplementary/ standalone information to support the operationalisation of this standard and is intended to be updated in line with changes to MSD's processes through time.

An identity referee is a person who:

- confirms the accuracy of information supplied by an individual
- confirms that, to their knowledge, the information supplied (e.g., biographic details or biometric information such as a photograph) belongs to that person

An authorised identity referee process may be undertaken if a client has no, or not enough identity documentation to be verified.

To be an authorised identity referee, the referee must:

- have a valid NZ Passport or NZ Driver Licence,
- have known the client for one year or more,
- not be related to the client or their extended family,
- not be the client's spouse or partner, and
- not live at the same address as the client.

The referee must be able to provide the above information to be considered an authorised identity referee.

Referee examples may include (but are not limited to):
Council Chairman
School Principals
Registered Teacher
Ministers of Religion
Doctors
Departmental officers
Well known officers of local welfare organisations
Justice of the Peace
Member of the Police
Kaumātua
Member of Parliament

MSD Survey Standard

Approved by: Privacy Security Oversight Board (PSOB)

Approval date: 15 June 2022

Next review: 15 June 2024

Standard Owner: General Manager Information

Introduction

The Ministry of Social Development ("the Ministry") often surveys clients, staff, stakeholders, and the public to help inform insights into our performance or areas for improvement around projects, programmes and initiatives being undertaken.

Surveys may be undertaken by the Ministry alone, in partnership with another organisation, or by a third party creating and conducting surveys on the Ministry's behalf.

This Standard is intended to provide guidance to Business Units who may undertake or facilitate surveys on the Ministry's behalf, and to set out the basic requirements that must be met.

1 Standard

1.1 Applicability

- 1.1.1 This Standard **must** be applied by any Business Unit that conducts or facilitates a survey.
- 1.1.2 Surveys **must** only collect information classified at 'Unclassified' and 'In-Confidence', in accordance with MSD's Information Classification Standard.
- 1.1.3 The Information Group **must** be consulted immediately if, for any reason, a survey relates to information classified above 'In-Confidence' (i.e., 'Sensitive' or 'Restricted').

1.2 Definitions

- 1.2.1 "Survey" means research questions on one or more topics, to which people are invited to voluntarily respond to for the purposes of gaining insights.
- 1.2.2 "Personal information" is any information about a specific individual. The information does not need to name the individual, if they are identifiable in other ways, like through their home address (it does not include a company, or a Trust, or an NGO).
- 1.2.3 "Collection" includes collection by phone, mail, email, the internet, in person, on social media, or through a specialised survey tool.
- 1.2.4 "Bias" is an inclination or prejudice for or against one person or group, especially in a way that could be considered to be unfair.
- 1.2.5 "Discrimination" is an unjust or prejudicial treatment of different categories of people, especially on the grounds of race, age, sex, or disability.
- 1.2.6 "Responses" to questions may be yes or no, on a scale, multi-choice, or free text.
- 1.2.7 "Conducting" a survey includes (but is not limited to):

- creating survey questions
- choosing participants
- distributing the survey
- collecting responses
- storing responses
- analysing responses
- sharing responses or analysis of responses with others (whether inside the Ministry or externally)
- disposing of responses.

2 Meeting the Standard

2.1 Demonstrating compliance

- 2.1.1 Compliance with this Standard **must** be clearly documented and agreed by the Control Owner or relevant Manager responsible for the Survey.

2.2 Purpose and collection

- 2.2.1 The Business Unit **must** document a clear purpose for the survey and the rationale for each survey question and associated collection of information from participants.
- 2.2.2 The Business Unit **must** engage the Information Group to review survey questions **if** any personal information is likely to be collected.
- 2.2.3 Prior to conducting any survey participants **must** have the purpose for collection and use of information explained to them.

2.3 Transparency and consent

- 2.3.1 Participation in all surveys **must** be voluntary, and it **must** be clear that participation is voluntary.
- 2.3.2 There **must** be clear, relevant, and accessible information made available for all participants in advance of their consenting to participate.
- 2.3.3 At a minimum, the information **must** make clear:
- what the purpose of the survey is
 - that participation is voluntary and that a decision not to participate will not affect a prospective participant's relationship with the Ministry
 - whether responses will be kept anonymous or whether the participant will be identifiable
 - how responses will be used by the Ministry or by others
 - who will view the responses (e.g., if they are to be shared with other organisations, which organisations will view the responses)
 - what will happen to the survey responses on completion of the survey (e.g., analysis, storage, destruction, etc.)
 - **[if personal information is being collected]** that those individuals have the right to access and correct information collected about them; and that they are provided with appropriate MSD contact information.

2.4 Anonymising surveys

- 2.4.1 Where identifying an individual is not necessary, there **must** be a process in place to ensure that no personal information is collected. Surveys **must not** include free-text fields for this purpose.
- 2.4.2 If surveys need to include free-text field the Information Group **must** be consulted for guidance.
- 2.4.3 Where identifying an individual is not necessary, the participants of the survey **must** be advised not to enter any personal information into the survey.
- 2.4.4 There **must** be a documented process for removing and destroying any unexpected collection of personal or identifiable information that participants supply in response to the survey, as per the Ministry's Information Retention and Disposal Standard.
- 2.4.5 Where identifying an individual is necessary, but their personal information is not necessary for research and evaluation, there **must** be a process in place to ensure that the information is de-identified.
- 2.4.6 Where participants need to create a profile or log-in to use a survey tool, usernames and passwords **must** meet the MSD Password Standard.

2.5 Research and Evaluation responsibilities

- 2.5.1 Surveys with the **explicit** purpose of Research and Evaluation **must** have their survey questions reviewed by the Research and Evaluation team to reduce the risk of unintended bias or discrimination. [An Ethics assessment form must be completed and sent to the Information Group.](#)
- 2.5.2 Consistent with 2.4, if personal information is collected from surveys, it **must** be de-identified after relevant research and evaluation purposes are met.
- 2.5.3 If analysis of a survey creates or reveals data capable of identifying an individual, the Privacy team **must** immediately be contacted for advice.

2.6 Tool selection

- 2.6.1 The method or tool used for publishing or submitting the survey **must** be certified and accredited, with its use approved by the Ministry and the Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO). The [Information Group can be contacted](#) to confirm a method or tools certification status.
- 2.6.2 The method or tool used **must** be appropriate for the purpose intended and be used in the way for which it has been approved. Some tools have been approved at MSD Enterprise level. See 3.2 for further details and their accompanying patterns to ensure use is consistent with Information Group expectations.

2.7 Managing bias and discrimination

- 2.7.1 Care **must** be taken to ensure that the end-to-end conduct of surveys does not introduce bias or discrimination at any point. Bias or discrimination may be introduced through the creation of inappropriate survey questions, the selection of participants, the distribution of surveys, access to surveys, and the analysis and implementation of survey responses.
- 2.7.2 If surveys have the potential to include or introduce any bias or discrimination, or it is uncertain if they will, the survey **must** be reviewed end to end by the Information Group to minimise any potential risk.
- 2.7.3 Where surveys produce results that are (or appear to be) biased or discriminatory, steps **must** be taken to identify and remove or mitigate the unintended bias or discrimination.



The problems we are trying to solve

We **mishandle** data by over-collecting, misusing, and keeping it too long

Poor data security exposes us to **breaches** (theft, deletion, alteration, misuse)

People do not have **transparency, control and choice** over their information

The **wrong person** accesses information they shouldn't

A **person is harmed** through a breach.

We share information with third parties **without appropriate safeguards**

Trust and confidence in MSD's reputation is eroded

External drivers and influences

The obligations we need to meet

Legislation

Privacy Act 2020

Public Records Act 2005

Māori-Crown relationship and Treaty obligations

Social Security Act 2018

Government regulations, strategies and guidance

Privacy Maturity Assessment Framework

Data Protection & Use Policy

Algorithm Charter for Aotearoa/NZ 2020

Privacy Maturity Assessment Framework (PMAF)

Self-assess privacy practices

Improve data handling

Build trust and compliance

Meet legal requirements

Strategic context

MSD's Enterprise Outcomes and Strategic Shifts

Tauāki Whakamaunga Atu Statement of Intent 2022 – 2026 – Outcomes

New Zealanders get the support they require

New Zealanders are resilient and live in inclusive and supportive communities

New Zealanders participate positively in society and reach their potential

Strategic Shifts for Te Pae Tawhiti (Our Future)

Mana manaaki
A positive experience every time

Kotahitanga
Partnering for greater impact

Kia takatū tātou
Supporting long-term social and economic development

Strategies for Privacy

Information, Data and Analytics (ID&A) Strategy

We use information fairly and respectfully, ensure its safe management and protection, and maintain its quality for effective decision-making.



Privacy in context

Key focus areas for Privacy

Education and awareness to advance a privacy aware culture

Transparency & Trust

Individual Access & Control

Responsible Data Use

Protecting Information

Safe Information Sharing

What this means for our customers



Align MSD's strategic and service requirements with the regulator's expectations.



Monitor and ensure that MSD continues to meet our specific privacy and information security responsibilities.



Provide privacy and risk advice that informs decisions and delivery of digital solutions and MSD services; to ensure these meet MSD requirements and our privacy and security responsibilities.



Design and risk assess business change and investment. Provide timely assurance that change(s) to digital solutions is delivered appropriately and responsibly.



MSD kaimahi are made aware of, and are supported to meet, privacy and information security expectations.



Privacy requirements enable MSD to safely and responsibly share information so clients receive the right services.



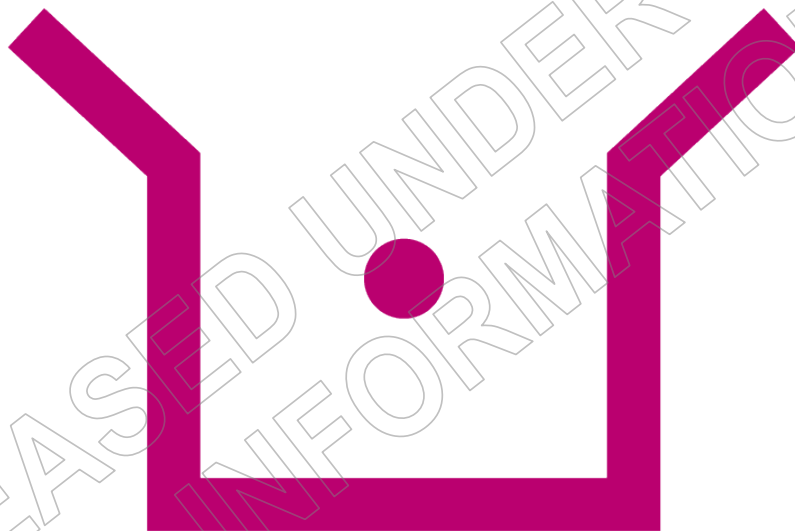
Privacy and risk outcomes enable digital solutions and MSD service improvements. Clients have trust and confidence their information is managed appropriately.



How we'll get there

	Do NOW	Do NEXT	Do LATER
IGART	<ul style="list-style-type: none"> Safeguard Individual Rights and Enable Data Access Implement training and education to raise Privacy Awareness 	<ul style="list-style-type: none"> Strengthen Data Breach Prevention, Response and Notification Enhance Transparency when collecting PII Privacy Governance, Assurance and Reporting Undertaken 	<ul style="list-style-type: none"> Manage Data Retention and Disposal/Deletion Effectively
LIP2	<ul style="list-style-type: none"> Uplift Third-Party Use and Sharing through appropriate safeguards Facilitate Efficient Consent Management ADM 	<ul style="list-style-type: none"> Implement Data Minimisation Practices Enforce Purpose Limitation Principle 	<ul style="list-style-type: none"> Embed Maori Data Rights
Other (IST, ID&A, ISART, etc)	<ul style="list-style-type: none"> Establish Robust Security and Safeguards 	<ul style="list-style-type: none"> Improve Data Accuracy and Quality 	<ul style="list-style-type: none"> Derive quality insights from PII to inform future decisions and improve client wellbeing

Information, Security and Identity
Te Rōpū Tiakina



Security, Privacy, Human Rights & Ethics Assessment

[Insert name]

Report Data

Name of Initiative	
Business Owner	Choose an item.
Stakeholder(s)	[Name, Title]
Objective ID	
Reference Documents	<ul style="list-style-type: none"> • [Include list of related docs with Objective references] • EG Privacy Analysis [insert Objective reference] • EG Full PHRaE report [insert Objective reference] • EG related system Certifications [insert Objective reference] • Appendix 3: Technical Context (available on request) [insert Objective reference] • Appendix 4: Privacy Analysis (available on request) [insert Objective reference] • Appendix 4: Privacy, Human Rights & Ethics Tool Report (available on request) [insert Objective reference]

Document History			
Author / Reviewer	Date	Version	Description

Overview

Description of Initiative
[Provide a summary of what they are doing and why, including what outcomes they are trying to achieve]

Nature of Information being handled	
[Overview of the types of information involved in the initiative i.e., is it medical information, aggregated data, identifiable information about singular individuals, identifiable information about groups of individuals, information about family / sexual violence, etc.]	
Information Classification:	Choose an item.
Impact if Confidentiality breached:	Choose an item.
Consequence if confidentiality is breached as [insert rationale].	
Impact if Integrity breached:	Choose an item.
Consequence if integrity is breached as [insert rationale].	
Impact if Availability breached:	Choose an item.
Consequence if availability is breached as [insert rationale].	

Summary of business process / information flows
<p>[Outline of the processes involved in the initiative, might just be a high-level description naming the processes, or could be more detailed descriptions of the processes themselves, the complexity and what is required to inform the risk assessment.</p> <p>MUST include a data / information flow diagram showing the flow of information within MSD systems and between MSD and third parties. If one is not available from the project Privacy / Security team must create it – separate guidance to be provided.]</p>

Description of systems	
[Include a summary of the systems that will be involved in the initiative. Should specify what internal systems are impacted as well as any external agency systems interacted with, cloud systems, information transfer / sharing mechanisms. Include a description of the nature of the changes to existing system/s.]	
Geographic location of information:	
Nature of Cloud service model:	Choose an item.
Independent Certifications:	[note N/A not a cloud service if not cloud]
Publicly Accessible:	Choose an item.

Scope	
Security	Choose an item.
<p>[Insert scope summary making clear what business processes/systems are within scope and what is excluded. Where the scope is limited, make sure it is clear what was covered and what was not.</p> <p>Scope may be limited for a range of reasons, but the main ones will be:</p> <ol style="list-style-type: none"> 1) the initiative relates to a type of system where the risks are well understood and there are standard controls that mitigate these risks, so we are validating the controls only, and 2) the initiative is relatively low risk and therefore we are focussing on only specific risks. If "other" is selected note the rationale and specific limitation.] 	
Privacy	Choose an item.
<p>[Insert scope summary making clear what business processes are within scope and what is excluded. Where the scope is limited, make sure it is clear what was covered and what was not. Make sure you specify the boundaries of the process that are within scope.</p> <p>Scope may be limited for a range of reasons, but the main ones will be:</p> <ol style="list-style-type: none"> 1) the initiative relates to a type of process where the risks are well understood and there are standard controls that mitigate these risks, so we are validating the controls only, 2) the initiative is relatively low risk and therefore we are focussing on only specific risks or principles, 3) the initiative sits alongside a business as usual process where some / many of the IPPs are already dealt with, and the initiative does not change these; the assessment will focus only on what is changing. If "other" is selected note below the rationale and specific limitation.] 	
Human Rights and Ethics	Choose an item.
<p>[Insert scope summary making clear what business processes are within scope and what is excluded. Where the scope is limited, make sure it is clear what was covered and what was not.</p> <p>Scope may be limited for a range of reasons, but the main ones will be:</p> <ol style="list-style-type: none"> 1) the initiative relates to a type of process where the risks are well understood and there are standard controls that mitigate these risks, so we are validating the controls only, 2) the initiative is relatively low risk and therefore we are focussing on only specific risks or principles, 3) the initiative sits alongside a business as usual process where some / many of the IPPs are already dealt with, and the initiative does not change these; the assessment will focus only on what is changing. If "other" is selected note below the rationale and specific limitation.] 	
Information Management	Choose an item.

[Insert scope summary making clear what business processes are within scope and what is excluded. Where the scope is limited, make sure it is clear what was covered and what was not]

Scope may be limited for a range of reasons, but the main ones will be 1) the initiative relates to a type of process where the risks are well understood and there are standard controls that mitigate these risks so we are validating the controls only, 2) the initiative is relatively low risk and therefore we are focussing on only specific risks or principles, 3) the initiative sits alongside a business as usual process where the assessment will focus only on what is changing. If "other" is selected note below the rationale and specific limitation.]

[For information management ensure the scope is specific to that function only and does not replicate scope that may already be covered by the other functional areas noted above]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Summary of Findings

Security

Insert high level summary of key findings, including specifying any contextual information about the solution, or areas where there is significant risk at go (live do not repeat the risk commentary though). For example, note where components are unsupported, or where demand for system has increased beyond expectations, or whether future improvements are anticipated. **Delete this section if not within scope.**

Privacy

Insert high level summary of key findings, including specifying those areas that could be contentious but that are mitigated. For example, specify the areas that we have confirmed there is legal authority or that we have confirmed that new share is in line with AISA requirements. **Delete this section if not within scope.**

Human Rights

Insert high level summary of key findings, including specifying those areas that could be contentious but that are mitigated, or areas where there is significant risk at go-live. For example, specify that there is discrimination present but that this is justified and why; demonstrating that the initiative has been designed to take account for this and this risk is "designed out." **Delete this section if not within scope.**

Ethics

Insert high level summary of key findings, including specifying those areas that could be contentious but that are mitigated, or areas where there is significant risk at go-live. **Delete this section if not within scope.**

Information Management

[Insert high level summary of key findings, including specifying those areas that could be contentious but that are mitigated, or areas where there is significant risk at go-live. For example, where information ownership is unclear, so we are seeking approval from GM Information as is allowed for under the Retention & Disposal Standard. **Delete this section if not within scope. As per scope ensure that for Information Management only those specific findings unique to IM are covered, and do not replicate other functional area findings.**

Compliance to Standards

Standard	Compliant	Comment (Comments and link to remediation plan required where not compliant)
Information Classification Standard	Yes / No	
Data Jurisdiction Standard	Yes / No	
Privileged Access Management Standard	Yes / No	
Third Party Assurance Standard	Yes / No	
Identity Governance Standard	Yes / No	
Automated Decision-Making Standard	Yes / No	
Information Retention and Disposal Standard	Yes / No	
Minimum Metadata Capture Standard	Yes / No	
Authentication Standard	Yes / No	
LDAP Directory Standard	Yes / No	
Encryption Standard	Yes / No	
Key Management Standard	Yes / No	
Patch Management Standard	Yes / No	
Vulnerability Management Standard	Yes / No	
Service Security Baseline Standard	Yes / No	
Remote Access Standard	Yes / No	
Password Standard	Yes / No	
Delete the following if not applicable		
Recording Standard	Yes / No	
Low Risk Website Standard	Yes / No	
Survey Standard	Yes / No	
Information Migration Standard	Yes / No	
Function Transfer Standard	Yes / No	
Digital Information Standard	Yes / No	

Risks

Risk Profile

Overall, there are [# very high risks, # high risks, # medium risks, # low risks and # very low risks – delete those that don't apply] associated with [insert name]. The risk profile below summarises the risks which are detailed in the risk assessment in Appendix 1.

All risks met their target residual risk level / # risks met their target residual risk level but # did not due to controls that were not fully effective. Target residual risk is the level of residual risk anticipated after the remediation of ineffective or partially effective controls. The # key controls that mitigate the identified risks were assessed and [found to be effective / # were found to be ineffective / partially effective]. A remediation plan has been agreed for all controls that were not fully effective. When evidence of effectiveness is provided this assessment will be updated. OR a remediation plan has been agreed for certain controls, however some control gaps will not be remediated, and the current residual risk should be accepted. The details of the control assessment activities are included in Appendix 2.

[Keep this commentary generic, further discussion should be in the next section]

		CONSEQUENCE				
		Routine	Minor	Moderate	Major	Severe
LIKELIHOOD	Almost Certain					
	Likely					
	Possible			R##		
	Unlikely		R##		R##	
	Rare					
KEY: Target Residual Risk: R## Current Residual Risk: R## Target Residual Risk = Current Residual Risk: R## Security Risks: SR## Privacy Risks: PR## Human Rights Risks: HR## Ethics Risks: ER## Information Management Risks: IMR##						

Commentary on Risk Profile

[If target risk is met in all cases delete this section]

Additional controls have been recommended to reduce [X of the Y] the risks further, and a remediation plan has been agreed. [Include comments about the number of controls requiring remediation and that actions have been agreed per Appendix 2.]

AND / OR

There are additional controls that could be implemented to reduce [X of the Y] risks further, but there are no plans to do so as [it these do not reflect current Ministry practice / it is cost prohibitive etc...] and this risk need to be accepted.

[Include comments about any controls that we would expect to see but that are not being implemented and why not – should tie to Appendix 2 analysis.]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Remediation Plan		
The table below outlines the agreed remediation activities . The control details, including results of assessment activities are included in Appendix 2.		
Control Ref & Title	Agreed Remediation Activities	Impacted Risks
	[Copy from Appendix 2 table, including control owner and timeframe]	R##, R##
The table below outlines those controls that cannot be assessed until after go-live, as the evidence will not exist until then.		
Control Ref & Title	Evidence to be provided	By When
	[include from who]	
The table below outlines those controls that are ineffective, but for which there are no immediate plans to remediate. The control details, including results of assessment activities are included in Appendix 2.		
Control Ref & Title	Rationale for not remediating	
	[Copy from Appendix 2 table]	

Approvals

Certification	
<input type="checkbox"/> Certified <input type="checkbox"/> Qualified Certification <input type="checkbox"/> Not Certified	
Comments	
<p>[If some controls cannot be assessed until system / process is live, note here the controls that require evidence and by when. Depending on the significance of these controls consider whether full or qualified certification should be given.</p> <p>Comment on any enterprise controls that are not going to be in place and why not. Note that the Current Residual Risk in these areas needs to be accepted.]</p>	
<div> <div>Hannah Morgan, Chief Information Security Officer / Chief Privacy Officer</div> <div>Date</div> </div> <p><i>I confirm that this report accurately represents the security and privacy risks associated with the identified scope and that the controls relied upon in this assessment are in place and operating at the time this certification was provided.</i></p>	

Accreditation	
<input type="checkbox"/> Accredited <input type="checkbox"/> Qualified Accreditation <input type="checkbox"/> Not Accredited	
Comments	
<p><i>I accept the current residual risks as outlined in this report and I confirm that the remediation plan (if any) will be implemented within the indicated timeframes.</i></p>	
Choose an item.	Date

Appendix 1 – Risk Assessment

Security Risk Assessment

The table below details the information security risks identified based on the effect they have on the confidentiality, integrity, and availability of Ministry data. The controls in **bold** are the key controls and have the strongest effect on reducing risk. The control detail and results of assessment of control effectiveness is outlined in Appendix 2.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
SR01	<p>Risk Title</p> <p>[Something Happens... for example an incident or a natural disaster or data leak happens – more examples can be found in the Risk Catalogue (A12035849)]</p> <p>[Due to ... for example a malicious party performs a malicious activity, or a Ministry admin misconfigure something – more examples can be found in the Risk Catalogue (A12035849)]</p> <p>KEEP EACH LINE TO NO MORE THAN ONE PAGE</p> <p>This may result in:</p> <ul style="list-style-type: none"> Choose an item. Choose an item. <p>Example Scenario(s): <This could be an actual example scenario(s) that could potentially happen if this risk is not mitigated></p> <ul style="list-style-type: none"> <p>Affects:</p> <p><input type="checkbox"/> Confidentiality, <input type="checkbox"/> Integrity, <input type="checkbox"/> Availability</p>	<p>Risk</p> <p>(consequence / likelihood)</p> <p>[colour cell according to risk rating]</p>	<p>[Insert list of controls – Please refer to the Control Catalogue to choose the appropriate controls best suited for this risk.</p> <p>Key controls are those that have the most significant impact on reducing risk and represent the minimum controls you would want to see. Key controls should be bold and highlighted in green: control.</p> <p>This list should include, and <i>Current Residual Risk</i> should be assessed on the basis of, controls that are assessed as (per Appendix 2):</p> <ul style="list-style-type: none"> Effective Not Yet Assessed (evidence does not exist until after go-live) Not Assessed (Not Key Control) <p>Not Assessed (Enterprise Control)]</p>	<p>Risk</p> <p>(consequence / likelihood)</p> <p>[colour cell according to risk rating]</p>	<p>Plans in place to remediate:</p> <p>The controls listed below have agreed remediation plans in place, and as such have been considered in assessing the Target Residual Risk. [delete if not applicable]</p> <p>[Insert list here]</p> <p>No plans in place to remediate:</p> <p>The controls listed below would reduce risk further, but there are no plans to remediate. As such they have not been considered in assessing the Target Residual Risk. [delete if not applicable]</p> <p>[Insert list here]</p> <p>[As this report should be populated from the beginning of a project, the list of required / anticipate controls should initially be listed in the “current controls” column so that this can be shared with the project. Later on, when assessment activities are complete, controls found to not be effective can be moved to this column.]</p>	<p>Risk</p> <p>(consequence / likelihood)</p> <p>[colour cell according to risk rating]</p>	<p>[Where applicable please provide a statement to support the reduction in risk as a result of the controls. (Note any specific controls which add particular weight to the risk reduction).</p> <p>Format example:</p> <ul style="list-style-type: none"> The consequence is reduced by... The likelihood is reduced by...

Privacy Risk Assessment

The table below details the privacy risks identified based on the effect they have on the alignment with the principles of the Privacy Act. The controls in **bold** are the key controls and have the strongest effect on reducing risk. The control detail and results of assessment of control effectiveness is outlined in Appendix 2.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
PR01	<p>Risk Title</p> <p>[Cause... what is the action or event that could lead to the risk... Risk... what may happen... Effect ... what would the impact be to your objective if it occurred]</p> <p>Affects:</p> <p>IPP1, IPP2, IPP3, IPP4, IPP5, IPP6, IPP7, IPP8, IPP9, IPP10, IPP11, IPP12 [delete all those not relevant]</p>	<p>Risk (consequence / likelihood)</p> <p>[colour cell according to risk rating]</p>	<p>[Insert list of controls – Think about the controls that are likely to make a material difference to reducing the consequence or likelihood of the risk occurring; do not just list everything they are doing.</p> <p>Key controls are those that have the most significant impact on reducing risk and represent the minimum controls you would want to see. Key controls should be bold and highlighted in green: control.</p> <p>This list should include, and <i>Current Residual Risk</i> should be assessed on the basis of, controls that are assessed as (per Appendix 2):</p> <ul style="list-style-type: none"> Effective Not Yet Assessed (evidence does not exist until after go-live) Not Assessed (Not Key Control) <p>Not Assessed (Enterprise Control)]</p>	<p>Risk (consequence / likelihood)</p> <p>[colour cell according to risk rating]</p>	<p>Plans in place to remediate:</p> <p>The controls listed below have agreed remediation plans in place, and as such have been considered in assessing the Target Residual Risk. [delete if not applicable]</p> <p>[Insert list here]</p> <p>No plans in place to remediate:</p> <p>The controls listed below would reduce risk further, but there are no plans to remediate. As such they have not been considered in assessing the Target Residual Risk. [delete if not applicable]</p> <p>[Insert list here]</p> <p>[As this report should be populated from the beginning of a project, the list of required / anticipate controls should initially be listed in the "current controls" column so that this can be shared with the project. Later on, when assessment activities are complete, controls found to not be effective can be moved to this column.]</p>	<p>Risk (consequence / likelihood)</p> <p>[colour cell according to risk rating]</p>	<p>[Where applicable please provide a statement to support the reduction in risk as a result of the controls. (Note any specific controls which add particular weight to the risk reduction). Format example:</p> <ul style="list-style-type: none"> The consequence is reduced by... The likelihood is reduced by...

RELEASED UNDER THE ACCESS TO INFORMATION ACT

OFFICIAL INFORMATION

Human Rights & Ethics Risk Assessment

The table below details the Human Rights and Ethical risks identified. The controls in **bold** are the key controls and have the strongest effect on reducing risk. The control detail and results of assessment of control effectiveness is outlined in Appendix 2.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
HRE01	Risk Title [Cause... what is the action or event that could lead to the risk... Risk... what may happen... Effect ... what would the impact be to your objective if it occurred]	Risk (consequence / likelihood) [colour cell according to risk rating]	[Insert list of controls – Think about the controls that are likely to make a material difference to reducing the consequence or likelihood of the risk occurring; do not just list everything they are doing. Key controls are those that have the most significant impact on reducing risk and represent the minimum controls you would want to see. Key controls should be bold and highlighted in green: control . This list should include, and <i>Current Residual Risk</i> should be assessed on the basis of, controls that are assessed as (per Appendix 2): <ul style="list-style-type: none"> Effective Not Yet Assessed (evidence does not exist until after go-live) Not Assessed (Not Key Control) Not Assessed (Enterprise Control)] 	Risk (consequence / likelihood) [colour cell according to risk rating]	Plans in place to remediate: The controls listed below have agreed remediation plans in place, and as such have been considered in assessing the Target Residual Risk. [delete if not applicable] [Insert list here] No plans in place to remediate: The controls listed below would reduce risk further, but there are no plans to remediate. As such they have not been considered in assessing the Target Residual Risk. [delete if not applicable] [Insert list here] [As this report should be populated from the beginning of a project, the list of required / anticipate controls should initially be listed in the "current controls" column so that this can be shared with the project. Later on, when assessment activities are complete, controls found to not be effective can be moved to this column.]	Risk (consequence / likelihood) [colour cell according to risk rating]	[Where applicable please provide a statement to support the reduction in risk as a result of the controls. (Note any specific controls which add particular weight to the risk reduction). Format example: <ul style="list-style-type: none"> The consequence is reduced by... The likelihood is reduced by...

RELEASED UNDER THE ACCESS TO INFORMATION ACT

Information Management Risk Assessment

The table below details the Information Management risks identified. The controls in **bold** are the key controls and have the strongest effect on reducing risk. The control detail and results of assessment of control effectiveness is outlined in Appendix 2.

#	Risk Description	Inherent Risk	Current Controls	Current Residual Risk	Future Controls	Target Residual Risk	Rationale
IM01	<p>Risk Title</p> <p>[Something Happens ... for example data is not transmitted due to format incompatibilities, data migrated is not covered by a current Disposal Authority – more examples can be found in the Risk Catalogue (A15657774)]</p> <p>This may result in:</p> <ul style="list-style-type: none"> Information retained for too long Non compliance with the Public Records Act or the Privacy Act Stakeholders lose confidence in the system Reputation Damage to MSD more examples can be found in the Risk Catalogue (A15657774) <p>Example Scenario(s): <This could be an actual example scenario(s) that could potentially happen if this risk is not mitigated></p> <ul style="list-style-type: none"> 	<p>Risk (consequence / likelihood) [colour cell according to risk rating]</p>	<p>[Insert list of controls – Think about the controls that are likely to make a material difference to reducing the consequence or likelihood of the risk occurring; do not just list everything they are doing.</p> <p>Key controls are those that have the most significant impact on reducing risk and represent the minimum controls you would want to see. Key controls should be bold and highlighted in green: control.</p> <p>This list should include, and <i>Current Residual Risk</i> should be assessed on the basis of, controls that are assessed as (per Appendix 2):</p> <ul style="list-style-type: none"> Effective Not Yet Assessed (evidence does not exist until after go-live) Not Assessed (Not Key Control) Not Assessed (Enterprise Control)] 	<p>Risk (consequence / likelihood) [colour cell according to risk rating]</p>	<p>Plans in place to remediate:</p> <p>The controls listed below have agreed remediation plans in place, and as such have been considered in assessing the Target Residual Risk. [delete if not applicable] [Insert list here]</p> <p>No plans in place to remediate:</p> <p>The controls listed below would reduce risk further, but there are no plans to remediate. As such they have not been considered in assessing the Target Residual Risk. [delete if not applicable] [Insert list here]</p> <p>[As this report should be populated from the beginning of a project, the list of required / anticipate controls should initially be listed in the "current controls" column so that this can be shared with the project. Later on, when assessment activities are complete, controls found to not be effective can be moved to this column.]</p>	<p>Risk (consequence / likelihood) [colour cell according to risk rating]</p>	<p>[Where applicable please provide a statement to support the reduction in risk as a result of the controls. (Note any specific controls which add particular weight to the risk reduction). Format example:</p> <ul style="list-style-type: none"> The consequence is reduced by... The likelihood is reduced by...]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Appendix 2 – Controls

The table below provides details of the controls relied upon in the risk assessment above, the results of assessment activities to determine whether key controls are effective, and any agreed remediation activities where controls are not effective. The details of the control assessment activities, including why certain controls were not selected for assessment, can be found in the Control Assessment Report.

#	Control Description	Control Validation Activities Completed	Control Effectiveness	Agreed Remediation Activity (where control ineffective / partially effective)
C01	Title [should match risk table, highlight title green if key control] [include description of control] Control Owner: [Insert name, title]	[include details of activities completed to validate controls and the results of those activities]	Choose an item. [colour the cell accordingly]	Choose an item. [IF Evidence to be provided after go-live THEN insert description of what evidence is expected, from who and by when. IF Remediation agreed with responsible manager, THEN insert summary of agreed remediation actions; these must be committed to by the responsible manager, do not include recommendations IF No plans to remediate - consistent with other Ministry systems THEN insert description of why this will not be remediated and what the Ministry standard is in this area. (E.g., cost prohibitive, vendor issue, enterprise known issue) IF No plans to remediate - Enterprise project underway THEN insert summary of enterprise project scope and anticipated completion date.] Responsible Manager: [Name, Title – may not be the control owner] Agreed Implementation Date: Click or tap to enter a date. [If control has not been assessed, leave this blank]

RELEASED UNDER
OFFICIAL INFORMATION ACT

Forms

Home (/dashboard) › Forms (/dashboard) › IT Security Forms (/dashboard#form-category-13) ›
Privacy or IT Security Incident Form (/forms/new?form_template_public_name=Privacy+or+IT+Security+Incident+Form)

Privacy or IT Security Incident Form

About this form

Privacy Incident

Notification form

Use this form when you have identified:

- personal information has been (or may have been) verbally, physically or electronically disclosed or used without authority
- personal information has been (or may have been) inappropriately collected
- following a request for personal information, a decision about whether to provide has not been made and communicated within 20 days (or extended timeframes)
- theft, or loss of personal information (e.g. files, USB sticks)
- unauthorised access to personal information
- correction or accuracy principles have not been applied correctly

This includes situations where there has been a close call or a near miss.

If you need help completing this form:

- Contact your manager
- Contact: PrivacyOfficer@msd.govt.nz

Users

Who is this on behalf of?

Name

Start typing to search for a user in (

Details

Business Group *

**When did the
incident happen? ***

Enter in the format
dd/mm/yyyy

**When was the
incident
discovered? ***

Enter in the format
dd/mm/yyyy

What personal information was involved? *

None selected ▼

Other, please specify

How did the incident occur? Explain in as much detail as possible. *

Do not include staff names

Do you consider this an isolated or systemic event? *

Please select ▼

How many people had their privacy compromised? *

What processes or safeguards were available? Were they followed? E.g. passwords, email quarantine, auto-populate turned off, attachments double-checked *

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Are you aware of any risk of harm or safety issues to any individual as a result of the incident? If yes, please explain? *

Is there any current media attention?

Please select

If yes, please state the media organisation and publishing date.

If no, do you anticipate any possible media attention?

If this relates to information of which we have lost control, has the information been retrieved, or an attempt made to retrieve the information?

If yes, please explain how this was done, by who and the outcome.

What action, if any, has been taken to prevent a similar incident occurring?

Other serious factors for consideration (e.g. risk to safety of individual or others):

Is the affected party aware of the incident?

Please select 

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Who received the information?

E.g. another client, a minister's office, a staff member, members of the public, media, reporters, contracted service providers, unknown recipient. Please provide details if known

Has the recipient acted on the information? For example, contacted the media, disclosed it to someone else or used it against the affected individual?

☐ **I am authorised to submit this form**

SUBMIT

Cancel (/)

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

	Consequence				
Category	1	2	3	4	5
Type of harm	-Potential for feeling disappointment, loss of control or autonomy, alienation -Little to no inconvenience to clients	-Potential for identity theft -Potential for financial loss -Inaccurate information provided to third party which needs to be corrected	-Potential for hurt, humiliation or reputational damage -Breach of access to/ correction of information provisions in the Privacy Act -Threats of harm other than physical harm -Significant inconvenience caused to clients (e.g. lost applications or documents)	-Potential for harassment such as doxing -Potential for actual physical harm e.g. disclosure of address to a violent ex-partner -Actual identity theft - Actual loss of business, employment or other opportunities -Actual financial loss that is not serious -Significant distress caused to clients -Actual discrimination or bias	-Actual hurt, significant humiliation or reputational damage -Actual physical or psychological harm -Actual serious financial or economic harm (e.g. denial of entitlement, denial of house)
Sensitivity of information	No sensitivity e.g. name, email	Limited sensitivity e.g. address, phone number* <i>(*note that address, phone and other details can be sensitive in some contexts e.g. if we know the information was released to an abusive ex-partner)</i>	Some sensitivity e.g. records of discrete interactions with MSD	Sensitive information e.g. bank account records, details of benefit history, gang affiliations	Most sensitive information e.g. criminal record, violence, details of abuse, medical records OR -Majority of personal information held by MSD about the relevant individual(s) is breached
Mitigations (including protection by a security measure)	Already remediated e.g. email recipient contacted and agreed to delete, all data encrypted using up to date encryptions standards	Mostly remediated, e.g. system patch in place, staff training refreshed, new locks in place, identity fraud is locked down in accordance with standard MSD guidance	Somewhat remediated e.g. altered data has been reversed, damaged corrected, or lost data found	Limited remediation possible e.g. assigning different identifiers, engaging credit bureau assistance providers, adding passwords to affected accounts	No actions yet taken due to system or other constraints OR no actions possible to reduce harm e.g. third party hacker OR mitigation was unsuccessful or ineffective
Recipient of breached personal information	Known individual(s) received the information/ had access to the information	Individual identities not known but the categories or boundaries of recipients is known an relatively small cohort e.g. <250 members of the Service Delivery region received the information OR all recipients are cooperative	Mostly known recipients, but it is possible or likely others may have received the personal information OR substantial cohort of recipients (<1,000) Possible breach of code of conduct by <10 Ministry staff or contractors	Unknown person(s) or known but uncooperative person(s) Likely breach of code of conduct by >10 Ministry staff or contractor	Known hackers/ extortionists Clear breach of code of conduct by Ministry staff or contractors
Number of individuals impacted	-Breach relates to one person or small number of people	-Breach relates to a small cohort (<250)	-Breach relates to a substantial cohort (<1,000)	-Breach relates to large cohort (1,000 <> 5,000)	-Widescale breach (> over 5,000 individuals) OR -Malicious insider breach
Duration of breach	-Breach occurred recently	-Breach occurred in the last week	-Breach occurred over the last few weeks	-Breach has occurred over weeks/ not been discovered for weeks	-Longstanding breach over months OR not known how long
Promptness of notification to Privacy Team	-Privacy team were notified within 72 hours of the breach	-Privacy team were notified after 72 hours but less than 1 weeks after the actual event(s)	-Privacy team were notified after 1 weeks but less than 2 weeks after the actual event(s)	-Privacy team were notified > 2 weeks after the actual event(s) but less than one month	-Privacy team were notified one or more months after the actual event(s)

Any red= escalate immediately to Privacy Lead, almost certainly notifiable to OPC and GM (except for promptness of notification to the Privacy Team, which is a matter of escalation and concern but not necessarily notification)

Any orange= escalate to Privacy Lead, likely notifiable (except for promptness of notification to the Privacy Team, which is a matter of escalation and concern but not necessarily notification)

Any yellow- discuss with senior privacy advisor, consider advising OPC even if not considered to meet the legal standard for notification, so OPC are aware for any direct approaches from

Any green- log and discuss mitigations with business as per the usual guidance/ process

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

	Chance of harm				
Level of harm	Rare	Unlikely	Likely or probable harm which is mitigated	Likely	Possible
5					
4					
3					
2					
1					

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

(date)

Client Number: 000 000 000

(name)

Address Line 1

Address Line 2

ADDRESS LINE 3

Dear (preferred name/salutation as per SWIFTT/UCVII)

Acknowledgement of your Privacy Act Request

Thank you for your request for personal information under the Privacy Act 2020 dated **[date]**. In that request you asked for: **[Insert information requested]**

We can confirm that we hold the information you request. We will prepare the information for you and provide it as soon as possible, and at the latest by **[date]** **[20 working days from the date of the request - See OPC website <https://www.privacy.org.nz/> for the response calculator]**.

If you have any further questions please do not hesitate to contact me on **[Phone]**.

Yours sincerely,

[Click here and type your name]

[Click here and type job title]

(date)

Client Number: 000 000 000

(name)

Address Line 1

Address Line 2

ADDRESS LINE 3

Dear (preferred name/salutation as per SWIFTT/UCVII)

Declining your Request for Information

Thank you for your Privacy Act request of [date] for: **INSERT WHAT THEY REQUESTED.**

Following a thorough search of our records, we are respectfully declining your request under section 53(a) of the Privacy Act 2020 because the information requested does not exist or, despite reasonable efforts to locate it, cannot be found.

If you wish to discuss this matter further, please contact me on [phone number].

Under section 70 of the Privacy Act 2020, you have the right to have this decision reviewed by the Office of the Privacy Commissioner. You can do this by completing an online form at <https://privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/complaint-self-assessment/> or writing to:

Office of the Privacy Commissioner
PO Box 10 094
The Terrace
Wellington 6143

Yours sincerely

[Click **here** and type your name]

[Click **here** and type job title]

(date)

Client Number: 000 000 000

(name)

Address Line 1

Address Line 2

ADDRESS LINE 3

Dear (preferred name/salutation as per SWIFTT/UCVII)

Our Response to your Information Request

Thank you for your request of (date) for: **INSERT WHAT THEY HAVE REQUESTED in italics or in quote marks**

We **enclose** our response to your request.

When you review the response, you will notice that some information has been removed from certain documents. **[We have also removed some pages of information in full].**

This information has been removed in accordance with the following section/s of the Privacy Act 2020:

Insert relevant sections and explanations here - See second page

If you wish to discuss this matter further, please contact me on (phone number).

Under section 70 of the Privacy Act 2020, you have the right to have this response reviewed by the Privacy Commissioner. You can do this by completing an online form:

<https://privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/complaint-self-assessment/>

Or you can write to:

Office of the Privacy Commissioner
PO Box 10 094
The Terrace
Wellington 6143

Yours sincerely

[Click here and type your name]

[Click here and type job title]

DELETE FROM FINAL COPY

- Section 53(b)(i) – disclosure would involve the unwarranted disclosure of the affairs of another individual.
- Section 53(c)(i) – disclosure would be likely to prejudice the maintenance of the law.
- Section 49(1)(a)(i) – disclosure would be likely to pose a serious threat to the life, health or safety of any individual.
- Section 49(1)(a)(ii) – disclosure would create a significant likelihood of serious harassment of an individual.
- Section 49(1)(b) – disclosure would be likely to prejudice the physical or mental health of the requestor.
- Section 49(1)(c) – disclosure would be contrary to the interests of the requestor, who is under the age of 16.
- Section 53(d) – disclosure would breach legal professional privilege.

(date)

Client Number: 000 000 000

(name)

Address Line 1

Address Line 2

ADDRESS LINE 3

Dear (preferred name/salutation as per SWIFTT/UCVII)

Our Response to your Information Request

Thank you for your request of [date] for: **INSERT WHAT THEY HAVE REQUESTED**
in italics or in quote marks

We **enclose** our response to your request.

If you wish to discuss this matter further please contact me on [telephone
number].

Under section 70 of the Privacy Act 2020, you have the right to have this response reviewed by the Privacy Commissioner. You can do this by completing an online form at <https://privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/complaint-self-assessment/> or writing to:

Office of the Privacy Commissioner
PO Box 10 094
The Terrace
Wellington 6143

Yours sincerely

[Click **here** and type your name]

[Click **here** and type job title]

Enc.[as appropriate]

(date)

Client Number: 000 000 000

(name)

Address Line 1

Address Line 2

ADDRESS LINE 3

Dear (preferred name/salutation as per SWIFTT/UCVII)

Extension to our Response Time

Thank you for your request for your personal information of [date]. You asked for: [INSERT information requested].

I am writing to notify you that we need to extend the time period for responding to your request. The reason for the extension is because [DELETE ONE: Either] your request is for a large amount of information and meeting our original time limit would unreasonably interfere with our operations. [OR] we need to consult with other parties about our decision on your request and we are unable to do this within our original time limit.

Our response will now be made by [specify date - make sure it is both reasonable under the circumstances and achievable, because you can only extend once.] We apologise for any inconvenience caused.

If you wish to discuss this matter further, please contact me on [telephone number].

Under section 70 of the Privacy Act 2020, you have the right to have this decision reviewed by the Privacy Commissioner. You can do this by completing an online form at <https://privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/complaint-self-assessment/> or writing to:

Office of the Privacy Commissioner
PO Box 10 094
The Terrace
Wellington 6143

Yours sincerely

[Click here and type your name]

[Click here and type job title]

(date)

Client Number: 000 000 000

(Contact name)
Agency address

Dear (name)

Transfer of Privacy Act Request

We received a Privacy Act 2020 request from [Requester's name] on [date] for:

[Insert request or part of request that needs to be transferred]

We have looked for the information requested and we do not hold it, however we believe that this information may be held by your agency or is more closely connected with the functions or activities of your agency.

We are therefore transferring this request under section 43 of the Privacy Act 2020 to [agency] for response. We have notified [Requester's Name] on [date] to inform them of the transfer.

If you wish to discuss this matter further contact me on [telephone number].

Yours sincerely

[Click here and type your name]

[Click here and type job title]

Enc. [Original request]

(date)

Client Number: 000 000 000

(name)

Address Line 1

Address Line 2

ADDRESS LINE 3

Dear (preferred name/salutation as per SWIFTT/UCVII)

Transfer of your Request for Information

Thank you for your request of [date] for INSERT WHAT THEY REQUESTED.

We do not hold the information you requested [about 'this particular thing' - if you are only transferring part of the request specify which part], however we believe this information may be held by another agency.

Under section 43 of the Privacy Act 2020, an agency may transfer a request if it is believed another agency holds the information or if the request is more closely associated with the functions of another agency.

We have therefore transferred [part of] your request to: [Insert the new agency].

You can expect [Agency] to respond to [this part of your request] you by [date (which is 20 working days after the day on which the request was received by the receiving agency)]. [We will respond to you about the remaining parts of your request by date].

If you wish to discuss this matter further contact me on [telephone number].

Under section 70 of the Privacy Act 2020, you have the right to have this decision reviewed by the Privacy Commissioner. You can do this by completing an online form at <https://privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/complaint-self-assessment/> or writing to:

Office of the Privacy Commissioner
PO Box 10 094
The Terrace
Wellington 6143

Yours sincerely

[Click here and type your name]

[Click **here** and type job title]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Contract Privacy Clauses

Contract Type	Privacy Clauses
Government Model Contract - Services	<p>Privacy</p> <p>14.1 Protection of Personal Information Where the Supplier has access to Personal Information under or in connection with this Agreement, the Supplier must:</p> <ul style="list-style-type: none"> a. only use, access, store, process or transmit that Personal Information to the extent necessary to provide the Deliverables or Services b. ensure that the Personal Information is protected against loss, access, use, modification, or disclosure that is not authorised by the Buyer, c. provide all information and assistance reasonably required by the Buyer to comply with its obligations under the Privacy Act in relation to this Agreement, and d. comply with the Privacy Act and not do anything under this Agreement that would cause the Buyer to breach the Privacy Act. <p>14.2 Privacy Breaches</p> <p>If the Supplier becomes aware of any Privacy Breach in relation to this Agreement it will notify the Buyer as soon as possible and take all reasonable steps:</p> <ul style="list-style-type: none"> a. to identify the person or persons affected, b. required by the Buyer to undertake its own investigation, c. stop, and/or mitigate the impact of, any Privacy Breach and prevent its reoccurrence, and d. the Supplier shall not notify any person of the Privacy Breach without the Buyer's prior written approval. <p>14.3 Application to Confidential Information The obligations under this clause 14 are not limited by and do not limit either Party's other obligations as regards the protection or security of Confidential Information set out in clause 13, provided that any disclosure of Confidential Information under clause 13.1 shall be subject to this clause 14.</p> <p>Definitions</p> <p>Personal Information has the meaning given to that term in the Privacy Act. Privacy Act means the Privacy Act 2020 and includes any codes or regulations issued under that Act.</p>

	<p>Privacy Breach means any:</p> <ul style="list-style-type: none"> • unauthorised or accidental access to or use of, or disclosure, alteration, loss, or destruction of any Personal Information; and • any action that prevents any Buyer from accessing Personal Information on either a temporary or permanent basis, whether or not: <ul style="list-style-type: none"> • caused by a person inside or outside of the Supplier; • attributable in whole or in part to any action by the Supplier; or • ongoing.
Government Model Contract - Goods	<p>Privacy</p> <p>14.1 Protection of Personal Information</p> <p>Where the Supplier has access to Personal Information under or in connection with this Agreement, the Supplier must:</p> <ol style="list-style-type: none"> a. only use, access, store, process or transmit that Personal Information to the extent necessary to supply the Goods, b. ensure that the Personal Information is protected against loss, access, use, modification, or disclosure that is not authorised by the Buyer, c. provide all information and assistance reasonably required by the Buyer to comply with its obligations under the Privacy Act in relation to this Agreement, and d. comply with the Privacy Act and not do anything under this Agreement that would cause the Buyer to breach the Privacy Act. <p>14.2 Privacy Breaches If the Supplier becomes aware of any Privacy Breach in relation to this Agreement it will notify the Buyer as soon as possible and take all reasonable steps:</p> <ol style="list-style-type: none"> a. to identify the person or persons affected, b. required by the Buyer to undertake its own investigation, c. stop, and/or mitigate the impact of, any Privacy Breach and prevent its reoccurrence, and d. the Supplier shall not notify any person of the Privacy Breach without the Buyer's prior written approval. <p>14.3 Application to Confidential Information The obligations under this clause 14 are not limited by and do not limit either Party's other obligations as regards the protection or security of Confidential Information set out in clause 13, provided that any disclosure of Confidential Information under clause 13.1 shall be subject to this clause 14.</p>

	<p>Definitions</p> <p>Personal Information has the meaning given to that term in the Privacy Act.</p> <p>Privacy Act means the Privacy Act 2020 and includes any codes or regulations issued under that Act.</p> <p>Privacy Breach means any:</p> <ul style="list-style-type: none"> • unauthorised or accidental access to or use of, or disclosure, alteration, loss, or destruction of any Personal Information; and • any action that prevents any Buyer from accessing Personal Information on either a temporary or permanent basis, whether or not: • caused by a person inside or outside of the Supplier; • attributable in whole or in part to any action by the Supplier; or • ongoing.
Outcome Agreement Framework Terms & Conditions	<p>8. Privacy of personal information</p> <p>8.1 To the extent that the Provider collects, uses, stores and/or discloses personal information related to the Outcome Agreement and Services, it will do so in accordance with:</p> <p>(a) the Privacy Act 2020 and any regulations issued under that Act;</p> <p>(b) any Law that amends or overrides any of the Information Privacy Principles of the Privacy Act 2020 and that applies to the Purchasing Agency or Provider; and</p> <p>(c) any Code of Practice or Approved Information Sharing Agreement (as defined in the Privacy Act 2020) that amends or overrides any of the Information Privacy Principles of the Privacy Act 2020 and that applies to the Purchasing Agency or Provider.</p> <p>8.2 Subject to clause 8.1, the Purchasing Agency and Provider will record in the Outcome Agreement, or any service specification attached to or referenced in the Outcome Agreement, the details of any personal information that will be shared by the Purchasing Agency with the Provider in connection with the Services, the purpose(s) for sharing and using the information and any agreement on the management (including security) of the information.</p> <p>8.3 Wherever a Provider supplies a privacy statement to clients in respect of the Services in accordance with Information Privacy Principle 3 of the Privacy Act 2020, the Provider will implement any reasonable directions made by the Purchasing Agency about the content of the privacy statement, including about the purpose(s) of collection and the disclosure of information.</p>

	<p>8.4 Before making a direction under clause 8.3, the Purchasing Agency will consult with the Provider about the proposed content of the privacy statement, and consider any reasonable issues or concerns raised by the Provider.</p> <p>8.5 In relation to any personal information provided or made available by the Purchasing Agency to the Provider in relation to the Outcome Agreement, the Provider will:</p> <ul style="list-style-type: none"> (a) ensure that the personal information is kept secure and protected by security safeguards that are reasonable in the circumstances to take against loss, access, use, modification or disclosure that is not authorised by the Outcome Agreement or any other misuse; (b) only use that personal information for the purposes set out in or authorised by the Outcome Agreement; (c) only transfer, disclose or allow access of that personal information outside of New Zealand with the Purchasing Agency's prior written consent; (d) provide all information and assistance reasonably required by the Purchasing Agency to comply with its obligations under the Privacy Act 2020; and (e) on termination or expiry of the Outcome Agreement, or on the Purchasing Agency's instructions, securely dispose of or return that personal information to the Purchasing Agency, except to the extent that such information is stored in electronic backups which cannot reasonably be extracted or deleted. <p>8.6 If the Provider becomes aware of any Security Breach (as defined below) in relation to the Outcome Agreement, it will notify the Purchasing Agency as soon as possible of that Security Breach and:</p> <ul style="list-style-type: none"> (a) promptly take such steps as are reasonably available to it to identify the person or persons involved in the Security Breach; (b) take reasonable steps to stop such Security Breach, to mitigate or contain the effects of the Security Breach, and to prevent its reoccurrence; (c) provide reasonable assistance to the Purchasing Agency in determining the extent of the Security Breach; (d) if the Purchasing Agency reasonably requests, assist the Purchasing Agency to undertake its own investigation in relation to the Security Breach; (e) will, if the Purchasing Agency reasonably requests: <ul style="list-style-type: none"> (i) assist the Purchasing Agency to notify affected individuals in relation to the Security Breach; and
--	--

- (ii) assist the Purchasing Agency to notify the New Zealand Privacy Commissioner in relation to the Security Breach, and the Provider acknowledges that it will not make any such notifications in relation to the relevant Security Breach without the Purchasing Agency's prior written approval (unless it is required to do so by applicable law); and
- (f) in such circumstances, the Purchasing Agency may require the Provider to immediately ensure that any person, third party supplier or subcontractor involved in causing the Security Breach is no longer engaged in providing the Services and that a suitably skilled, qualified and experienced replacement is engaged. For the purposes of this clause 8.6, Security Breach means any:
 - (a) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, any personal information; and
 - (b) any action that prevents either party from accessing the personal information on either a temporary or permanent basis (except disposal of that personal information in accordance with clause 8.5(e)), whether or not:
 - (c) caused by a person inside or outside of the Provider;
 - (d) attributable in whole or in part to any action by the Provider; or
 - (e) ongoing.

9. Confidentiality

9.1 Confidential Information

The Purchasing Agency and Provider each confirms that it has adequate security measures to safeguard the other party's Confidential Information from unauthorised access or use by third parties, and that it will not use or disclose the other party's Confidential Information to any person or organisation other than:

- (a) to the extent that the disclosure or use is:
 - (i) necessary to perform its obligations, or to exercise its rights, under or in relation to the Outcome Agreement (for example, to give effect to clauses 5.8 and 5.9 (Principles of Co-ordination and Cooperation), 8 (Privacy of personal information) and 11.4(e) (Orderly Transition of Services) of these Framework Terms and Conditions); or
 - (ii) is expressly authorised by the Outcome Agreement;
- (b) if the other party gives prior written approval to the use or disclosure;

(c) if the use or disclosure is required by law (including under the Official Information Act 1982) or parliamentary convention; or

(d) in relation to disclosure, if the information has already become public, other than through a breach of the obligation of confidentiality by one of the parties.

9.2 Confidentiality undertaking required

(a) If these Framework Terms and Conditions or the Outcome Agreement permit disclosure of any Confidential Information to any third party (including any auditor or reviewer appointed under clauses 5.4 or 5.5), the Provider and the Purchasing Agency (as applicable) may only disclose that Confidential Information to that third party if it first obtains a written confidentiality undertaking from that third party in terms substantially similar to those set out in this clause.

(b) To avoid doubt, Personnel of the Purchasing Agency or Provider are not third parties for the purpose of clause 9.2(a). Each party may disclose Confidential Information to Personnel who need to know such information for the purposes of the Outcome Agreement, provided each party ensures that its Personnel:

- (i) are aware of the confidentiality obligations in these Framework Terms and Conditions and the Outcome Agreement; and
- (ii) do not disclose or use Confidential Information except as allowed by these Framework Terms and Conditions and the Outcome Agreement

11.6 Survival

Clauses 5.4 (Special Enquiry Rights), 7 (Dispute Resolution), 8 (Privacy of personal information), 9 (Confidentiality), 10 (Intellectual Property), 11.4 (Termination), 12 (Recovery, Reduction or Suspension of Payments), 13 (Indemnity), 15 (General Terms) and Schedule One (Definitions and Interpretation) all survive termination or expiry of the Outcome Agreement.

13. Indemnity

13.1 The Provider indemnifies the Purchasing Agency against all losses suffered or incurred by the Purchasing Agency as a result of any claim by a third party that:

- (a) the possession or use of any Intellectual Property Rights supplied or licensed by the Provider to the Purchasing Agency or used to provide the Services infringes a third party's Intellectual Property Rights; or

	<p>(b) a third party's rights (including privacy rights) have been breached as a consequence of the Provider's breach of the Outcome Agreement, including these Framework Terms and Conditions.</p> <p>13.2 The indemnity in clause 13.1 applies to the extent that any relevant loss was not caused by the Purchasing Agency's negligence, breach of the Outcome Agreement or willful misconduct.</p> <p>Definitions</p> <p>Confidential Information means information that: (a) is by its nature confidential; (b) is marked by either party as 'confidential', 'in confidence', 'restricted' or 'commercial in confidence'; (c) is provided by either party or a third party 'in confidence'; (d) either party knows or ought to know is confidential; or (e) is of a sensitive nature or commercially sensitive to either party, and includes personal information (as defined in the Privacy Act 2020)</p>
Registration of Interest Terms	<p>4.9 Notification of outcome During the 30 Business Days after the Contract has been signed, the Buyer:</p> <ul style="list-style-type: none"> a. will let all unsuccessful Respondents know the name of the Successful Respondents, if any b. may make public the name and address of the Successful Respondents (if any) and any unsuccessful Respondents c. will publish a Contract Award Notice on GETS, where applicable. Contract Award Notices are available to view by the public on GETS. The Respondent may request that the Buyer withhold its address from the Contract Award Notice for privacy reasons. The Buyer may withhold the Respondent's address from the Contract Award Notice in a manner consistent with the Privacy Act 2020. <p>4.15 Confidential Information</p> <ul style="list-style-type: none"> a. Without limiting any other confidentiality agreement between them, the Buyer and the Respondent will both take reasonable steps to protect the other party's Confidential Information. b. Except as permitted by the other provisions of this Section 4.15, neither party will disclose the other party's Confidential Information to a third party without that other party's prior written consent. c. Each party may each disclose the other party's Confidential Information to anyone who is directly involved in the ROI process on that party's behalf, but only for the purpose of participating in the ROI. This could include (but is not limited to) officers, employees, consultants, contractors,

	<p>professional advisors, evaluation panel members, partners, principals or directors. Where this occurs, the disclosing party must take reasonable steps to ensure the third party does not disclose the information to anyone else, and does not use the information for any purpose other than participating in the ROI process.</p> <p>d. The Respondent acknowledges that the Buyer's confidentiality obligations are subject to requirements imposed by the Official Information Act 1982 (OIA), the Privacy Act 2020, parliamentary and constitutional convention, and any other obligations imposed by law. Where the Buyer receives an OIA request that relates to a Respondent's Confidential Information, the Buyer will consult with the Respondent and may ask the Respondent to explain why the information is considered by the Respondent to be confidential or commercially sensitive.</p> <p>e. The Respondent may disclose the Buyer's Confidential Information to the extent strictly necessary to comply with law or the rules of any stock exchange on which the securities of the Respondent or any related entity are currently listed. Unless prohibited by law, the Respondent must consult with the Buyer before making such a disclosure.</p> <p>f. The Buyer will not be in breach of its obligations if it discloses Confidential Information to the appropriate authority because of suspected collusive or anti-competitive tendering behaviour</p>
Request for Quotes Terms and Conditions	<p>5.11 Notification of outcome During the 30 Business Days after the Contract has been signed, the Buyer:</p> <p>a. will let all unsuccessful Respondents know the name of the Successful Respondents, if any</p> <p>b. may make public the name and address of the Successful Respondents (if any) and any unsuccessful Respondents</p> <p>c. will publish a Contract Award Notice on GETS, where applicable. Contract Award Notices are available to view by the public on GETS. The Respondent may request that the Buyer withhold its address from the Contract Award Notice for privacy reasons. The Buyer may withhold the Respondent's address from the Contract Award Notice in a manner consistent with the Privacy Act 2020.</p> <p>5.17 Confidential Information</p> <p>a. Without limiting any other confidentiality agreement between them, the Buyer and the Respondent will both take reasonable steps to protect the other party's Confidential Information.</p>

	<p>b. Except as permitted by the other provisions of this Section 5.17, neither party will disclose the other party's Confidential Information to a third party without that other party's prior written consent.</p> <p>c. Each party may each disclose the other party's Confidential Information to anyone who is directly involved in the RFQ process on that party's behalf, but only for the purpose of participating in the RFQ. This could include (but is not limited to) officers, employees, consultants, contractors, professional advisors, evaluation panel members, partners, principals or directors. Where this occurs, the disclosing party must take reasonable steps to ensure the third party does not disclose the information to anyone else, and does not use the information for any purpose other than participating in the RFQ process.</p> <p>d. The Respondent acknowledges that the Buyer's confidentiality obligations are subject to requirements imposed by the Official Information Act 1982 (OIA), the Privacy Act 2020, parliamentary and constitutional convention, and any other obligations imposed by law. Where the Buyer receives an OIA request that relates to a Respondent's Confidential Information, the Buyer will consult with the Respondent and may ask the Respondent to explain why the information is considered by the Respondent to be confidential or commercially sensitive.</p> <p>e. The Respondent may disclose the Buyer's Confidential Information to the extent strictly necessary to comply with law or the rules of any stock exchange on which the securities of the Respondent or any related entity are currently listed. Unless prohibited by law, the Respondent must consult with the Buyer before making such a disclosure.</p> <p>f. The Buyer will not be in breach of its obligations if it discloses Confidential Information to the appropriate authority because of suspected collusive or anti-competitive tendering behaviour.</p>
Request for Proposal Terms and Conditions	<p>6.11 Notification of outcome</p> <p>During the 30 Business Days after the Contract has been signed, the Buyer:</p> <p>a. will let all unsuccessful Respondents know the name of the Successful Respondents, if any</p> <p>b. may make public the name and address of the Successful Respondents (if any) and any unsuccessful Respondents</p> <p>c. will publish a Contract Award Notice on GETS, where applicable. Contract Award Notices are available to view by the public on GETS. The Respondent may request that the Buyer withhold its address from the Contract Award Notice for privacy reasons. The Buyer may withhold the</p>

	<p>Respondent's address from the Contract Award Notice in a manner consistent with the Privacy Act 2020</p> <p>6.17 Confidential Information</p> <p>a. Without limiting any other confidentiality agreement between them, the Buyer and the Respondent will both take reasonable steps to protect the other party's Confidential Information.</p> <p>b. Except as permitted by the other provisions of this Section 6.17, neither party will disclose the other party's Confidential Information to a third party without that other party's prior written consent.</p> <p>c. Each party may each disclose the other party's Confidential Information to anyone who is directly involved in the RFP process on that party's behalf, but only for the purpose of participating in the RFP. This could include (but is not limited to) officers, employees, consultants, contractors, professional advisors, evaluation panel members, partners, principals or directors. Where this occurs, the disclosing party must take reasonable steps to ensure the third party does not disclose the information to anyone else, and does not use the information for any purpose other than participating in the RFP process.</p> <p>d. The Respondent acknowledges that the Buyer's confidentiality obligations are subject to requirements imposed by the Official Information Act 1982 (OIA), the Privacy Act 2020, parliamentary and constitutional convention, and any other obligations imposed by law. Where the Buyer receives an OIA request that relates to a Respondent's Confidential Information, the Buyer will consult with the Respondent and may ask the Respondent to explain why the information is considered by the Respondent to be confidential or commercially sensitive.</p> <p>e. The Respondent may disclose the Buyer's Confidential Information to the extent strictly necessary to comply with law or the rules of any stock exchange on which the securities of the Respondent or any related entity are currently listed. Unless prohibited by law, the Respondent must consult with the Buyer before making such a disclosure.</p> <p>f. The Buyer will not be in breach of its obligations if it discloses Confidential Information to the appropriate authority because of suspected collusive or anti-competitive tendering behaviour</p>
--	--

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:	October 2022
Next Review Date:	October 2024
Approved by:	Organisational Health Committee, October 2022
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 we respect people's privacy and human rights in an ethical manner. 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.

As we interact daily 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 we partner and share 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 we must uphold and maintain compliance with the New Zealand Privacy Act 2020.

Scope

This policy applies to all Ministry staff including contractors and partners; 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 only collects the information it needs from people, and is transparent and clear about its purpose and use

Any information we collect must be for a defined and intended purpose; limited to what is necessary and relevant to the Ministry's activities or a legislative purpose. When we collect information from people, we tell them, in a way that makes sense to them, what data or information is collected about them, how it is used, 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. Transparency is important for trust and respecting people's mana.

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

While delivering on our services, we leverage data to enhance customer experience and help us make better decisions for better lives and better outcomes. The data we use must be treated as an extension of the whānau, people, and communities that it was collected from, handling it with the deserving level of dignity, care, respect, and protection.

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

Incorporating diverse cultural interests, backgrounds, perspectives, and needs is key to building trust when we interact with our clients and each other. We are objective, fair, do not disadvantage others, and do not discriminate.

4. The Ministry shares personal information responsibly

As public servants, we recognise that information is a powerful enabler for creating actionable intelligence, and we leverage this taonga respectfully, ethically, and transparently. When we share the personal information of our clients and our people, it is for their benefit. We are committed to sharing only what is needed to fulfil that purpose or request.

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

The Ministry supports the choices of clients and staff when they make decisions about what personal information they want to share; and how they want it used and by whom. We encourage people to see what is collected and recorded about them and wherever possible give easy access to, and oversight 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 IT security, 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 that their teams are familiar with the Ministry's information policies, 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 • Reporting any IT security, information security or privacy incidents to their line manager
Information Asset Owners	<p>All information assets owners are responsible for ensuring that the risks to, and the opportunities for their information assets are managed and monitored. The information asset owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information.</p> <p>At MSD, Information Asset Owners will typically be DCE, Regional Commissioners or Group General Managers.</p>
Information Stewards	<p>Information stewards are responsible for the quality, integrity, and responsible use of information assets, enabling the organisation to gain maximum value from the information. They are also responsible for supporting information asset owners to make informed decisions about the management and use of their asset for the duration of its lifecycle.</p> <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 MSD, Information Stewards will typically be General Managers, Regional Directors and Directors.</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.</p>

Person/Party	Responsibility
	<p>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 MSD, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC) and the Technical Design Committee (TDC).</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 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 • 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 the Ministry staff or clients about possible privacy breaches • 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 • Overseeing the function governing what the Ministry can and cannot do with personal information. <p>At MSD, 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
Chief Analytics Officer	<p>The Chief Analytics Officer (CAO) oversees the analytics function, including data analytics and data science. They set strategic priorities for this function and identify new opportunities for the Ministry based on data.</p> <p>The CAO is responsible for:</p> <ul style="list-style-type: none"> Managing the analytics needs across the organisation The creation of data warehouses Data governance and data management frameworks <p>At MSD, the CAO is the GGM Insights.</p>
Information Group	<p>Information 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, 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 and comply with information legislation and related regulations. Delivering a foundational capability - providing direction, guidance tools, training and support to ensure information capability improvements can be achieved.
Insights	<p>The Insights Group is responsible for:</p> <ul style="list-style-type: none"> 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.
Ethics Advisor	<p>Responsible for formulating, reviewing, and disseminating ethics related documents, and providing guidance related to all ethical issues (code of conduct, conflicts of interest, outside activities, etc.)</p> <p>At MSD, 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 or thing in an unfair way, because of allowing personal opinions to influence your judgment.
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 we live, what we look like, what we think or what we believe. They are based on principles of dignity, equality, and mutual respect.
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, 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, or disclosing of personal information by secure means to other parties within the Ministry, or with other organisations, for certain purposes using approved information agreements.
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 you have to control your 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.

Template Information Sharing MOU

Introduction

MSD practice is that most forms of information sharing between MSD and another agency need to be formally documented, using an appropriate form of information sharing MOU, agreement or letter. The only exceptions to this are ad hoc, isolated information shares where the justification for sharing is clear and the sharing is quick and simple, e.g., over the phone to address a serious threat to a person's safety or responding to a specific request relating to an individual by email.

Attached to this cover sheet is MSD's template Information Sharing MOU.

When can it be used?

This template can be used in situations where MSD and another agency or organisation are sharing a significant amount of personal or other sensitive information, and there is an existing legal basis for the sharing. Its purpose is to record the sharing and set expectations and controls around how the information is to be shared and used. For example, MSD might be sharing a substantial dataset with another agency, or it might be disclosing information to another agency and/or obtaining information from another agency on a regular basis.

When should it not be used?

This template cannot be used to, and it does not, provide an independent legal basis for the sharing of personal information that is not otherwise permissible under the Privacy Act or specific statutory provisions. It needs to record the existing legal basis for the sharing, whether that be under the IPPs or specific statutory sharing provisions.

The template should also not be used for:

- sharing situations that are or will be covered by an approved information sharing agreement under the Privacy Act; or
- information sharing arrangements in the context of departmental host or shared services arrangements between MSD and another department or departmental agency.

Approved Information Sharing Agreements (AISAs) typically contain provisions detailing what must be in MOUs that parties enter into in reliance on the sharing authority established by the AISA. This template may not comply with those provisions or need to be amended to meet the requirements of the relevant AISA. Accordingly, we recommend early engagement with MSD Legal on MOUs that rely on an AISA as the justification for sharing.

How to use it

The details for a given MOU are entered into Schedule 1 (Administrative Details) and Schedule 2 (Information Sharing Schedule). Except for completing the MOU's title page and the other party's name on page 1, the front end of the MOU (i.e., the Background section and clauses 1-10) is intended to be common to all information-sharing MOUs. Drafting notes in blue provide guidance on the parts of the template that need to be completed, and on optional clauses you can include. All blue drafting notes and square brackets should be deleted before providing the MOU to the other party.

Who to ask for help

If you need help with completing the template, contact IP&S and/or MSD Legal. It is particularly important that the justifications for sharing set out in the MOU are legally correct. MSD Legal is ultimately responsible for ensuring the sharing is lawful and so must be consulted before the MOU is finalised and the sharing commences.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT



**MINISTRY OF SOCIAL
DEVELOPMENT**
TE MANATŪ WHAKAHIATO ORA

Memorandum of Understanding

Relating to the sharing of information for [insert brief description of purposes of sharing]

Ministry of Social Development

and

[Insert full name of the other party]

Document version control

Version	Signing Date	Summary of changes	Signed	
1		Not applicable.	Signed in the signature blocks further below.	
			MSD	[acronym for other party]
			(Signature) Name: Position:	(Signature) Name: Position:
			MSD	[acronym for other party]
			(Signature) Name: Position:	(Signature) Name: Position:
			MSD	[acronym for other party]
			(Signature) Name: Position:	(Signature) Name: Position:

Contents

1.	Term and effect of MOU	1
2.	Sharing and use of Specified Information for Specified Purposes	2
3.	Justifications for Sharing	2
4.	General responsibilities	3
5.	Security of information	3
6.	Dispute resolution	4
7.	Relationship management	5
8.	Termination	5
9.	Amendments	6
10.	Definitions and interpretation	6
	Schedule 1: Administrative Details	9
	Schedule 2: Information Sharing Schedule	10

Memorandum of Understanding

Parties

Ministry of Social Development (**MSD**)

and

[Insert full name of the other party] ([insert acronym for other party])

Background

- 1 The parties wish to share specific kinds of information for specific purposes and have agreed in this MOU upon the parameters within which such sharing may occur. The context for the sharing is set out in Appendix 1 (Administrative Details).
- 2 The MOU may cover one or more flows of information between the parties (these are called Information Flows) and is designed to be expanded over time for additional flows through the insertion of additional Appendixes to Schedule 2 (Information Sharing Schedule).
- 3 The information that may be shared within an Information Flow is called Specified Information and the purposes for which that Specified Information may be shared and used in the context of the particular flow are called Specified Purposes.
- 4 There needs to be a lawful basis for every Information Flow that covers the flow and use of the Specified Information for the Specified Purposes. This MOU calls that lawful basis a Justification for Sharing. The Justifications for Sharing are to be recorded alongside each Information Flow in the Appendixes to Schedule 2 (Information Sharing Schedule).
- 5 Capitalised terms have the meanings given to them in clause 10.

Terms

1. Term and effect of MOU

- 1.1 This MOU commences on the Start Date and will continue until the End Date (the **Term**), unless terminated earlier in accordance with clause 8. These dates are recorded in Schedule 1 (Administrative Details).
- 1.2 The parties may agree in writing to extend the Term at any time prior to expiry of the MOU.
- 1.3 The parties acknowledge that this MOU:
 - (a) is not a legally binding contract;
 - (b) is not an approved information sharing agreement under the Privacy Act 2020;
 - (c) does not authorise any breach of the Information Privacy Principles (**IPPs**) in that Act; and
 - (d) does not authorise any act or omission that would be contrary to law.

2. Sharing and use of Specified Information for Specified Purposes

2.1 The parties agree that:

- (a) all Information Flows, the Specified Information they cover, the Specified Purposes for each Information Flow, and the Justification(s) for Sharing for each Information Flow, need to be recorded in one or more Appendixes to Schedule 2 (Information Sharing Schedule);
- (b) the Information Flows as at the Start Date are recorded in the first Appendix to Schedule 2 (Information Sharing Schedule); and
- (c) if the parties wish to add further Information Flows, they will complete additional Appendixes to Schedule 2 as required which, once agreed, will form a part of this MOU.

2.2 The parties agree:

- (a) to share the Specified Information for the Specified Purposes as described in the Appendixes to Schedule 2 for each Information Flow, in accordance with the terms of this MOU; and
- (b) that all collections, uses and disclosures of Specified Information must be in accordance with all applicable law, including the Privacy Act 2020, the Human Rights Act 1993 and, where relevant, the Official Information Act 1982.

2.3 A party (the **Receiving Party**) may use Specified Information received from the other party (the **Disclosing Party**) for any Specified Purpose for which the information has been shared.

2.4 The parties will ensure that the Specified Information is only disclosed, collected, used and accessed by appropriately trained, qualified and authorised staff, contractors or third parties.

2.5 Subject to any further limitations set out in Schedule 2, the Receiving Party may only use Specified Information for a purpose other than a Specified Purpose (an **Other Purpose**), or disclose Specified Information to another agency, if the Receiving Party is permitted, authorised or required by law to do so. To avoid doubt, no further limitation set out in Schedule 2 will prevent a party from complying with applicable statutory duties.

3. Justifications for Sharing

3.1 The Justification(s) for Sharing for each Information Flow are set out in the Appendixes to Schedule 2 (Information Sharing Schedule).

3.2 If, at any time during the Term, either party no longer believes that a Justification for Sharing applies to a given Information Flow or that there has been a change in law, practice or government policy that affects the parties' ability to rely on the justification, that party will inform the other party promptly and the parties will meet as soon as practicable to assess:

- (a) whether the sharing remains lawful and appropriate;
- (b) whether the sharing should continue or cease;
- (c) whether the parties should consult the Office of the Privacy Commissioner; and
- (d) any other matters that either party considers relevant.

4. General responsibilities

4.1 Each party will comply with the other party's reasonable requirements relating to:

- (a) the methods and timing of requests for, and the sharing of, Specified Information;
- (b) technical standards that need to be followed in relation to the sharing of Specified Information;
- (c) access control, security and storage requirements that need to be implemented for the sharing of Specified Information;
- (d) quality checking of the Specified Information to be shared;
- (e) training of Authorised Personnel; and/or
- (f) how to deal with technical faults or corrupted data.

This clause 4.1 does not limit the requirements of any Justification for Sharing or the other terms of this MOU.

4.2 Without limiting clause 4.1, the parties may agree upon particular requirements of the kinds referred to above in an Appendix to Schedule 2 (Information Sharing Schedule) and, if they do, they will comply with them.

5. Security of information

5.1 Security measures

Each party:

- (a) will store information it receives under this MOU in a secure system that protects the information against unauthorised use, access, modification, destruction or disclosure;
- (b) will ensure that any data extraction programs and other processes used to obtain and transfer information under this MOU will only obtain and transfer information the parties have agreed to share and no other Personal Information;
- (c) agrees that all information shared in accordance with this MOU is confidential and will be shared by way of a secure encrypted exchange mechanism;
- (d) will ensure its contractors and employees handling information that is to be exchanged or has been exchanged under this MOU will comply with the Privacy Act and any other applicable law;
- (e) agrees to cooperate in any review of the performance or use of any online transfer mechanism used to share information under this MOU; and
- (f) will, if an alternative method to share information needs to be used because the primary method is not available or appropriate for a particular instance of sharing, use the alternative secure method specified in the applicable Appendix to Schedule 2, and ensure that that method protects the information against unauthorised use, access, modification, destruction or disclosure.

5.2 Privacy Breaches

- (a) If a party (**Party A**) becomes aware of or suspects there has been a Privacy Breach involving any Personal Information that the other party (**Party B**) has shared with Party A:

- (i) Party A will notify Party B as soon as possible and, in any event, within 24 hours or in accordance with other applicable regulation or legislation;
 - (ii) the parties will investigate the Privacy Breach to the extent they are able to do so, in accordance with their standard internal investigation processes;
 - (iii) each party will cooperate with the other in any such investigation and will provide such information and updates on the investigation as the other party may reasonably request; and
 - (iv) the parties will work together to manage the implications and consequences of the Privacy Breach.
- (b) Either party may suspend the sharing of any information under this MOU while the Privacy Breach is being investigated or remedied.
- (c) Except as stated in clause 5.2(d), neither party will comment publicly (including to the media) on the Privacy Breach if doing so could affect the other party without first consulting the other party.
- (d) If, under the Privacy Act 2020:
- (i) it is necessary to notify the Privacy Commissioner of the Privacy Breach and the Privacy Breach involves Personal Information that, under that Act, is deemed to be held by one party alone, then that party will be responsible for making the notification to the Privacy Commissioner and, if required, to affected individuals; or
 - (ii) it is necessary to notify the Privacy Commissioner of the Privacy Breach and both parties hold the same Personal Information, the party responsible for the Privacy Breach will be responsible for making the notification to the Privacy Commissioner and, if required, to affected individuals,
- and in either case the notifying party will use reasonable endeavours to discuss its proposed notification with the other party before notifying the Privacy Commissioner and (when required) the affected individual(s).

6. Dispute resolution

- 6.1 If either party becomes aware of a dispute relating to this MOU or its formation, that party will promptly advise the other party in writing of the dispute.
- 6.2 The parties' Relationship Managers will use their best endeavours to resolve the dispute within 20 working days of the receiving party's receipt of the notice referred to in clause 6.1.
- 6.3 If the parties' Relationship Managers are unable to resolve the dispute within the 20 working days referred to in clause 6.2, either party may by notice in writing to the other party escalate the dispute.
- 6.4 If a dispute is escalated under clause 6.3, the parties shall:
- (a) agree upon a written summary of the dispute, the issues involved, and the reason or reasons for the dispute not being resolved or, failing agreement on such a summary within 20 working days after the date of receipt of the notice of escalation, prepare separate written summaries within the next 10 working days; and

- (b) submit the summary or summaries to each party's chief executive or their nominated delegate within 30 working days after the date of receipt of the notice of escalation.
- 6.5 The parties' chief executives or their nominated delegates will meet as soon as practicable after their receipt of the summary or summaries to try to resolve the dispute.
- 6.6 In this clause 6, "chief executive" includes any equivalent position by a different name.

7. Relationship management

- 7.1 Each party must nominate a representative (the **Relationship Manager**) who will be:
 - (a) responsible for monitoring that party's compliance with this MOU; and
 - (b) the key contact person for:
 - (i) receiving notices issued under this MOU; and
 - (ii) any other matters relevant to this MOU.
- 7.2 The parties' Relationship Managers at the Start Date are specified in Schedule 1 (Administrative Details). A party may change its Relationship Manager at any time by written notice to the other party informing the other party of the change and the name and contact details of the replacement Relationship Manager.

8. Termination

- 8.1 Either party (the **first party**) may terminate this MOU or one or more Information Flows for cause, by written notice to the other party (the **second party**) with immediate effect on the date of termination specified in that notice, if:
 - (a) the second party commits a breach of this MOU that is incapable of being remedied; or
 - (b) the second party commits a breach of this MOU that is capable of being remedied, the first party has issued a written notice to the second party requiring it to be remedied, and the second party has not remedied the breach within 10 working days of its receipt of the notice.
- 8.2 If the parties have been unable to resolve a dispute within 50 working days after the date of receipt of the notice of escalation referred to in clause 6.3, either party may terminate this MOU on written notice to the other party.
- 8.3 Either party may terminate this MOU for convenience upon 30 days' written notice to the other party, but will give the other party an opportunity to comment on the proposed termination before sending the written notice.
- 8.4 Either party may terminate an Information Flow for convenience upon 30 days' written notice to the other party, but will give the other party an opportunity to comment on the proposed termination before sending the written notice.
- 8.5 The parties may at any time agree in writing to terminate this MOU or one or more Information Flows.

9. Notices

- 9.1 Notice under this MOU are to be made in writing and delivered to the other party's Relationship Manager (email being the preferred method of delivering notices).
- 9.2 A notice will be deemed to be received:
- (a) In the case of a letter sent at the Relationship Manager's postal address, on the fifth Working Day after posting;
 - (b) In the case of personal delivery, on receipt; and
 - (c) in the case of email at the time the email leaves the communication system of the sender, provided that the sender:
 - (i) does not receive any error message relating to the sending of the email at the time of the sending; and
 - (ii) has obtained confirmation that the email has been delivered to the recipient (which confirmation may be in the form of an automated delivery receipt from the communications system of the recipient).

on the day on which it is dispatched or; if dispatched after 5pm (in the place of receipt) on the next Working Day after the date of dispatch.

10. Amendments

- 10.1 If the parties wish to vary an Information Flow, they will agree upon the amendments to the relevant Appendix to Schedule 2, replace the original Appendix with the amended version, and record their agreement in the MOU's document control sheet.
- 10.2 If the parties wish to remove an existing Information Flow, they will either follow the process in clause 9.1 or, if all Information Flows in the relevant Appendix are being removed, agree upon removal of the Appendix, and record their agreement in the MOU's document control sheet.
- 10.3 If the parties wish to add new Information Flows, they will agree upon the content of a new Appendix to Schedule 2, attach that Appendix to the MOU, and record their agreement in the MOU's document control sheet.
- 10.4 All other amendments to the MOU need to be agreed in writing and signed by authorised representatives of the parties.

11. Definitions and interpretation

Unless the context requires otherwise, the terms below have the meanings given to them:

Authorised Personnel means any Personnel who have access to Specified Information or other information provided by the other party;

End Date means the date on which this MOU will expire, as specified in Schedule 1, subject to earlier termination under clause 8 or extension of the Term under clause 1.2;

Information Flow means a flow of information between the parties as described in an Appendix to Schedule 2 (Information Sharing Schedule);

IPP means an Information Privacy Principle in section 22 of the Privacy Act 2020;

Justification for Sharing means the lawful basis for a party sharing Specified Information with the other party for Specified Purposes as described for each Information Flow in the Annexure(s) to Schedule 2 (Information Sharing Schedule);

MOU means this Memorandum of Understanding;

Personal Information means information about an identifiable individual;

Personnel means any employee, agent, or representative of the relevant party or any contractor of or provider of services to that party;

Privacy Breach means:

- (a) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, Personal Information; or
- (b) an action that prevents access to Personal Information on either a temporary or permanent basis;

Relationship Manager has the meaning in clause 7.1;

Specified Information means the specific kinds of information that the parties agree may be shared in accordance with and subject to the terms of this MOU, as described for each Information Flow in the Annexure(s) to Schedule 2 (Information Sharing Schedule);

Specified Purposes means the specific purposes for which the Specified Information may be shared in accordance with and subject to the terms of this MOU, as described for each Information Flow in the Annexure(s) to Schedule 2;

Start Date means the date on and from which the terms of this MOU apply, as specified in Schedule 1; and

Term has the meaning in clause 1.1.

Working Day has the meaning given in section 13 of the Legislation Act 2019.

Execution

SIGNED by the **Ministry of Social Development** by

SIGNED by **[insert name of other party]** by

Signature

Signature

Name

Name

Position

Position

Date

Date

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Schedule 1: Administrative Details

Introduction

This Schedule records administrative details relating to the operation of this MOU as referred to in the body of the MOU.

Details

Context of MOU (Background paragraph 1)	[Explain why this MOU is being put in place, to enable readers of the MOU to understand the relevant background/context.]			
Start Date (Clause 1.1)	[insert start date]			
End Date (Clause 1.1)	[insert start date]			
Relationship Managers (Clause 7.2)	Relationship Manager for MSD		Relationship Manager for [insert acronym for other party]	
	Name:	[insert name]	Name:	[insert name]
	Email:	[insert email]	Email:	[insert email]
	Phone:	[insert phone number]	Phone:	[insert phone number]
Additional terms	[If the parties require additional terms for a particular MOU, enter them here. Otherwise, state "None" or delete this row.]			

Schedule 2: Information Sharing Schedule

1. Introduction

- 1.1 The Appendixes to this Schedule record the Information Flows, and their Specified Information, Specified Purposes and Justification(s) for Sharing, as referred to in the MOU.
- 1.2 The Information Flows as at the Start Date are recorded in Appendix 1.
- 1.3 If the parties have added further Information Flows after the Start Date in accordance with clause 9.3, those additional flows will be recorded in additional Appendixes and form part of this MOU.

2. Appendixes

- 2.1 Attached.

Appendix 1: Information Flows as at Start Date of MOU

1. Introduction

1.1 This Appendix set out the Information Flows between the parties as at the Start Date of the MOU.

1.2 For each Information Flow:

- (a) there is a description of the Information Flow;
- (b) the direction(s) of flow of the Specified Information between the parties are identified;
- (c) the Specified Purposes for which the Specified Information may be shared and used are listed; and
- (d) the Justification(s) for Sharing are described.

2. Information Flows

[Instructions: It is important to complete the table below carefully and fully. All relevant details must be captured.]

An Information Flow is a flow of specified information between the parties for specified purposes. In the first column (Information Flow (description)), give a brief description of the flow. In the next column, specify the information elements that will be shared (e.g., name, address, etc) and how the information flows. For example, MSD might be sharing information elements A, B and C with Oranga Tamariki. In that case, you would specify elements A, B and C, and state MSD>Oranga Tamariki. In this example, if Oranga Tamariki were sharing other personal information with MSD, you would complete another row for that. In the Specified Purposes column be clear on the purposes for which the information is being shared and can be used. Purposes must be specific, not 'catch-alls'. In the Justification(s) for Sharing column, specify the legal basis for sharing the information. For example, the sharing might be justifiable under a specific exception in IPP11, or it might be justifiable under a specific statutory provision under, for example, the Social Security Act or the Tax Administration Act. You must be specific about the justification, i.e., you cannot simply say something like "IPP11" or "Social Security Act".

If it assists with capturing the intention of the information sharing and flow, and one exists, it is acceptable to include an agreed flow or process diagram that helps inform the descriptions laid out in section 2.1.]

2.1 The Information Flows and their associated parameters are as set out below.

Information Flow (description)	Specified Information and direction(s) of flow	Specified Purposes	Justification(s) for Sharing (i.e., legal authority for sharing)
[Insert description] [For example: Details of MSD clients wanting referral to Oranga Tamariki]	[Specify information elements and direction of flow]	[State specific purposes for which information is being shared]	[State specific justification]

Information Flow (description)	Specified Information and direction(s) of flow	Specified Purposes	Justification(s) for Sharing (i.e., legal authority for sharing)
for their X service are collated/sent by x department at MSD to y department at Oranga Tamariki]	[For example: Name, address, phone number MSD > Oranga Tamariki]	[For example: To enable MSD clients to participate in X service and to enable Oranga Tamariki to become aware of and contact those clients, and provide them with service X.]	[For example: Authorisation is obtained from MSD clients via a consent form]

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

3. Other requirements and processes

3.1 The parties will comply with the other requirements and processes set out below.

Further limitations on use or sharing for Other Purposes (Clause 2.5 states that a receiving party may only use the Specified Information for a purpose other than a Specified Purpose (which it calls an Other Purpose) or disclose the Specified Information to another agency, if the Receiving Party is permitted, authorised or required by law to do so. But it also contemplates that the parties may agree on further limitations to such use or sharing for Other Purposes, even when lawful. If the parties have agreed on further limitations on how a receiving party can use or share Specified Information, they will be stated below.)	
Further limitations on use of Specified Information by Receiving Party for Other Purposes	<p>[If required, set out further limitations on uses for other purposes. If not required, enter "Not applicable".]</p> <p>EITHER [no use for other purposes without written consent – may be desirable where MSD wishes or the parties wish to control uses for other purposes]</p> <p>A Receiving Party must obtain the Disclosing Party's written consent before using Specified Information for a purpose other than a Specified Purpose (and under clause 2.5 the use must be permitted or authorised by law).</p> <p>OR [no use for other purposes without notification – may be desirable where MSD wishes or the parties wish to be notified if the information is used for another purpose]</p> <p>If a Receiving Party wishes to use any Specified Information for a purpose other than a Specified purpose, it must notify the Disclosing Party of the proposed use before using it for that purpose [optional: or, if not feasible, as soon as practicable afterwards] (and under clause 2.5 the use must be permitted or authorised by law).</p> <p>OR [no use for other purposes unless authorised, required by law, or permitted by law for health or safety reasons – may be desirable if MSD or the parties wish to limit other uses to the situations described]</p> <p>The Receiving Party will only use the Specified Information for Specified Purposes, unless use for another purpose is:</p> <ul style="list-style-type: none"> authorised in writing by the Disclosing Party [optional: or the individual to whom the Personal Information relates]; or required by law; or permitted by law for a purpose relating to the health or safety of any individual or the public. <p>OR [something else]</p> <p>[insert other limitations]</p>
Further limitations on disclosures of Specified Information by Receiving Party to third parties	<p>[If required, set out further limitations on disclosures to third parties. If not required, enter "Not applicable".]</p> <p>EITHER [no disclosure to third party without consent – may be desirable where MSD wishes or the parties wish to control disclosures to other parties]</p> <p>A Receiving Party must obtain the Disclosing Party's written consent before disclosing Specified Information to a third party (and under clause 2.5 the disclosure must be permitted or authorised by law).</p>

	<p>OR [no disclosure to third party without notification – may be desirable where MSD wishes or the parties wish to be notified of such disclosures]</p> <p>If a Receiving Party wishes to disclose any Specified Information to a third party, it must notify the Disclosing Party before doing so [optional: or, if not feasible, as soon as practicable afterwards] (and under clause 2.5 the disclosure must be permitted or authorised by law).</p> <p>OR [no disclosure to third parties unless authorised, required by law, or permitted by law for health or safety reasons – may be desirable if MSD or the parties wish to limit disclosures to the situations described]</p> <p>The Receiving Party will not disclose any Specified Information to a third party unless the disclosure is:</p> <ul style="list-style-type: none"> • authorised in writing by the Disclosing Party [optional: or the individual to whom the Personal Information relates]; or • required by law; or • permitted by law for a purpose relating to the health or safety of any individual or the public. <p>OR [no disclosure to researchers or analysts in reliance on IPP11 exceptions – may be desirable when the Specified Information is particularly sensitive]</p> <p>The Receiving Party will not, in reliance on the relevant exceptions in IPP11, allow researchers or analysts from other agencies or organisations to access the Specified Information for statistical or research purposes, regardless of whether the information will not be published in a form that could reasonably be expected to identify the individuals concerned.</p> <p>OR [something else]</p> <p>[insert other limitations]</p> <p>OR/AND</p> <p>If Inland Revenue is a party to the MOU, the following limitation will apply to MSD:</p> <p>MSD must not, without first obtaining Inland Revenue's written consent:</p> <ul style="list-style-type: none"> (a) transfer any Information outside of New Zealand or Australia; (b) make any Information available to any person outside of New Zealand; (c) allow any person to access Information from a location outside of New Zealand; or (d) permit or authorise any of the things described in (a) to (c) to occur
	<p>Particular requirements relating to handling of and access to Specified Information</p> <p>(The parties may agree to particular requirements regarding one or more of the matters below. If they don't, they can request each other to comply with reasonable requirements relating to these matters during the term of the MOU. See clause 4 (General responsibilities).)</p>
Methods and timing of requests for, and the sharing of,	EITHER

Specified Information	<p>[Enter details if required] [For example: SEEMail must be used for the transfer of Specified Information between the parties on weekly basis each Monday once xxx has completed.]</p> <p>OR</p> <p>No particular requirements specified at Start Date.</p>
Minimum technical standards that need to be followed	<p>EITHER</p> <p>[Enter details if required] [For example: Information is encrypted/password protected during transfer and while at rest.]</p> <p>OR</p> <p>No particular requirements specified at Start Date.</p>
Access control, security and storage requirements	<p>EITHER</p> <p>[Enter details if required]</p> <p>OR</p> <p>No particular requirements specified at Start Date.</p>
Quality checking of the Specified Information to be shared	<p>EITHER</p> <p>[Enter details if required]</p> <p>OR</p> <p>No particular requirements specified at Start Date.</p> <p>OR [if the legal authority for sharing the Specified Information is based on an individual giving consent to the sharing of their personal information]</p> <p>To the extent that the Justification for Sharing of Specified Information is based on IPP 11(1)(c) or other consent-based authority, prior to any exchange of information:</p> <ul style="list-style-type: none"> (a) The Disclosing Party will ensure that each individual who gives consent to sharing of Specified Information is provided with sufficient information to enable free and informed consent to be given. Such information shall include the nature of the information to be exchanged under this MOU; and (b) The Disclosing Party will seek and obtain the free and informed consent of the individual for the Disclosing Party for the Specified Purposes. That consent shall be recorded and retained by the Disclosing Party in a secure manner. <p>The Receiving Party may request (and the Disclosing Party shall supply) any reasonable information about the secure retention of consent checks in relation to the storage of consent forms during the term of the MOU.</p> <p>Where the Receiving Party is not satisfied with the result of any check on the storage of consent forms, the Receiving Party will contact the Disclosing Party Relationship Manager within five working days.</p>

Training of Authorised Personnel	<p>EITHER</p> <p>[Enter details if required]</p> <p>OR</p> <p>No particular requirements specified at Start Date.</p> <p>OR/AND</p> <p>If Inland Revenue is a party to the MOU, the following will be a requirement on MSD:</p> <p>Certificates of secrecy: MSD shall ensure that all its Authorised Personnel sign a certificate of confidentiality in the form prescribed by the Commissioner of Inland Revenue from time to time.</p>
How to deal with technical faults or corrupted data	<p>EITHER</p> <p>[Enter details if required]</p> <p>OR</p> <p>No particular requirements specified at Start Date.</p>
<p>Alternative / fall-back method for sharing information</p> <p>(Clause 5.1(f) states that the parties will, if an alternative method to share information needs to be used because the primary method is not available or appropriate for a particular instance of sharing, use the alternative secure method specified in the applicable Appendix to Schedule 2)</p>	
Alternative secure method for sharing information	<p>[For example: Encrypted USB stick]</p>

Personal Employment Information Policy

This page outlines the policy on staff and personnel records.

On this Page:

Purpose

Personal employment information is collected and held at Ministry offices in a confidential and secure manner for legal, administrative, salary payment, and staff management purposes. The Ministry has a duty to collect this information for a variety of purposes and must ensure that it complies with all relevant legislation (e.g. Employment Relations Act 2000, Income Tax Act 2004, Privacy Act 2020, Official Information Act 1982, Public Records Act 2005, and the Security in the Government Sector (SIGS) Manual 2002).

Personal employment information may be kept in different places and managed by different people across the Ministry, e.g. Managers or designated staff members, Payroll (National Office), and Human Resources.

The purpose of this policy is to set out the rights and responsibilities of the Ministry and staff in relation to the confidentiality, security, transfer, access, archiving and destruction of personal employment information.

Coverage

This policy applies to all personal employment information collected by the Ministry, which is held on but not limited to, the following files:

Personnel file

A Personnel file is created for each employee (permanent, fixed term, and casual) at the commencement of employment. Information held on this file relates to employment, performance, and management history. Personnel files must be managed and held in a secure location determined by the service line or business unit. When an employee leaves the Ministry, their personnel file is then transferred to Information Management (National Office) by the manager. Information Management hold and manage the file for at least 7 years after the last date of employment.

[Read more about managing personnel files. \[http //google/resources/helping_staff/procedures_manuals/hr/managing_personnel_files.html\]](http://google/resources/helping_staff/procedures_manuals/hr/managing_personnel_files.html)

Payroll file

A Payroll file is created for all Ministry employees. Information held on this file relates to any approved salary payment actions, including starting or ceasing employment, deductions or change in hours. Payroll files are managed and held for 7 years after the last date of action by Information Management (National Office).

Attendance records (timesheets) and leave forms

Attendance records and leave forms are filed as verification of time worked so that salary can be calculated and paid. Attendance records and leave forms must be managed and held in a secure location determined by the service line or business unit, for 18 months.

Recruitment file

A Recruitment file is opened for each new vacancy. Information held on this file relates to the recruitment or appointment process, including applications and other correspondence received or sent. If an appointment review is lodged against a provisional appointment, the file will also hold any documentation relating to the review. Recruitment files must be managed and held in a secure location determined by the service line or business unit for at least 12 months after the last date of action.

Dispute and personal grievance files

A dispute and personal grievance file is created when an employee lodges a dispute or personal grievance. Dispute and personal grievance files are managed and held by Human Resources for 7 years after the last date of action.

Confidentiality

Personal employment information is confidential information.

Those employees and managers who have access to personal employment information must maintain its confidentiality. A breach of confidentiality may result in disciplinary action.

Managers and designated support staff are responsible for the confidentiality of all personal employment information and files held at their site.

Security

Personal employment information must be stored, administered, transferred, and managed in a way that provides reasonable safeguards against loss, unauthorised access, and misuse.

Personal employment information must be held in a secure area with restricted access or stored in suitable lockable filing cabinets.

Personal employment information must not be left unattended on desks during the day and must be securely filed at the end of the day.

Care must be taken when transferring personal employment information so that the information is kept safe, secure, and confidential.

Access

Access to personal employment information held by the Ministry is restricted to the following:

Staff who, as part of their role, have delegated authority to collect, administer, and maintain this information (e.g. including but not limited to: Human Resources, Payroll, Audit staff, Records Services staff, Support staff, and Executive Assistants).

Managers with line reporting responsibility for the employees concerned.

Employees and managers who are selected to take part in recruitment and as part of that process view information supplied by applicants.

Government agencies who have a 'statutory power' to request such information.

An authorised agent of the employee.

The Privacy Act 2020 also provides that all employees are entitled to access their own personal employment information held by the Ministry either during or after employment. The Ministry may be entitled to withhold some of the information if a relevant exception in the Act applies.

Retention, archiving and destruction

The Ministry has a duty to retain personal employment information for a variety of purposes.

Personal employment information can only be destroyed or transferred to Archives New Zealand with approval from MSD Record Services.

The destruction of all personal employment information must be in accordance with a retention and disposal schedule authorised by Archives New Zealand (as required by the Public Records Act 2005) and Ministry Records Management policies and procedures. Advice on when you should archive or whether you can destroy information is available from MSD Records Services. [\[http://doogle/resources/helping_staff/policies_standards/hr/personal_grievances.html#top#top\]](http://doogle/resources/helping_staff/policies_standards/hr/personal_grievances.html#top#top)

Content owner: [Human Resources](#) Last updated: 15 November 2024