MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

22 December 2022

Tēnā koe

On 11 November 2022, you emailed the Ministry of Social Development (the Ministry) requesting, under the Official Information Act 1982 (the Act), the following information:

> *The following request applies for the timeframe from 1 January 2020 to the date of this request:*
>
> - *All Privacy Impact Assessments All privacy strategies, roadmaps, workplans Privacy Maturity Assessment Framework reports and results*
> - *All templates used for responding to privacy act requests and similar*
> - *All policies, standard operating procedures and guidance relating to privacy All privacy training modules or presentations delivered or created since 1 January 2020*
> - *This request applies to draft versions of the documents as well as finalized documents*

On 28 November 2022, we emailed you seeking refinement of your request due to the broad nature of what was being sought. You replied the same day confining the date range to between 1 June 2021 to 31 October 2022.

On 6 December 2022, we emailed you stating that more time was required to make a decision on your request in order to allow for consultations to occur. The timeframe on your request was extended to 23 December 2022.

For the sake of clarity, we will now respond to the parts of your request in-turn:

- *All Privacy Impact Assessments All privacy strategies, roadmaps, workplans Privacy Maturity Assessment Framework reports and results*

- *All templates used for responding to privacy act requests and similar All policies, standard operating procedures and guidance relating to privacy.*

Please see **Appendix One** which provides:

- The Ministry's *Security, Privacy, Human Rights & Ethics Triage* document template;
- The Ministry's *Security, Privacy, Human Rights & Ethics Assessment* template; *The Data Protection & Use Policy* document; and
- The *Privacy, Human Rights & Ethics Framework* document.

Please note that your request for guidance relating to privacy is very broad in scope, and substantial manual collation would be required to locate and prepare all documents within scope of your request. As such, I refuse your request under section 18(f) of the Act. The greater public interest is in the effective and efficient administration of the public service.

I have considered whether the Ministry would be able to respond to your request given extra time, or the ability to charge for the information requested. I have concluded that, in either case, the Ministry's ability to undertake its work would still be prejudiced.

- *All privacy training modules or presentations delivered or created since 1 January 2020*
- *This request applies to draft versions of the documents as well as finalized documents.*

The Ministry's Learning and Capability Group builds awareness and capability of our people through regular training which includes the Ministry's Privacy policy and procedures. For example:

- Through the Ministry's online induction training all employees are required to complete Code of Conduct training which references Information Management and Privacy and Security.

- On an annual basis all Ministry employees are required to complete online refresher training which includes Code of Conduct and Information Management, Privacy and Security.

- Ministry employees have access to the Office of the Privacy Commissioner learning modules Privacy ABC and the Privacy Act 2020.

- Staff who undertake the following NZQA qualifications are required to complete US19906 Demonstrate knowledge of information and privacy legislation in relation to the public sector:

- NZ Certificate in Public Sector Service Delivery (Level 4)
- NZ Zealand Certificate Regulatory Compliance (Core Knowledge) (Level3)

More details about these courses, in addition to the resources cited previously are provided in **Appendix Two**. Their titles are also listed here in order of appearance:

- Employee Induction Module Section 3 - Ministry expectations showing 3.5 privacy expectations and 3.6 mandatory module including assessment on Information Management, Privacy and Security
- Copy of Code of Conduct referencing Privacy Act 2020 pg 10; Accessing Information and Misuse of Information page 11
- Rise Module – Information Management, Privacy and Security
- Office of the Privacy Commissioner – a Quick tour of the privacy principles
- Office of the Privacy Commissioner – the Privacy Act 2020 Changes.

The principles and purposes of the Official Information Act 1982 under which you made your request are:

- to create greater openness and transparency about the plans, work and activities of the Government,
- to increase the ability of the public to participate in the making and administration of our laws and policies and
- to lead to greater accountability in the conduct of public affairs.

This Ministry fully supports those principles and purposes. The Ministry therefore intends to make the information contained in this letter and any attached documents available to the wider public. The Ministry will do this by publishing this letter on the Ministry's website. Your personal details will be deleted, and the Ministry will not publish any information that would identify you as the person who requested the information.

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 this response about privacy resources and training, 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,

Hannah Morgan
General Manager, Information

Appendix One

Security, Privacy, Human Rights & Ethics Triage

*The purpose of the document is to **confirm the approach to be taken** for security, privacy, human rights and ethics assessments and to **record the rationale supporting that approach**. Once completed this document will be retained by the Information Group and a **copy provided to the business / IT team** working on the initiative so that all parties are clear what approach is to be taken. This document **should be prepared by the Information Group** after initial engagement at the beginning of a project and should be **returned to the business / IT team within one week of initial discussions**. This document should be updated if significant changes to initiative design or scope are made.*

Initiative Overview

Name of Initiative:	
Key Contact (s):	
Portfolio:	[eg Employment / Income Modernisation etc]
Priority indicator:	[indicate whether this is a ministry priority and if so what the priority source and reference is eg PEC priority 3]
Go-Live date:	

Description of initiative

[High level 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 ie is it medical information, aggregated data, identifiable information about singular individuals, identifiable information about groups of individuals, information about family / sexual violence, etc etc]

[Information classification should reflect the classification of the information you expect to be involved in this initiative and should be discussed with the Information Management Team. NOTE: the system may end up being certified HIGHER than this, but it shouldn't be lower]

Information Classification:	Choose an item.

Summary of business process / information flows

[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, depending on where the design is at, the complexity and what is required to make decisions. Should also outline the information flows within MSD and between MSD and third parties. Include a high-level diagram if relevant / available. JUST INCLUDE WHAT YOU KNOW, YOU DON'T NEED TO HAVE A FULL UNDERSTANDING AT THIS STAGE; JUST NEED TO KNOW ENOUGH TO BE ABLE TO IDENTIFY THE SCOPE OF WORK TO BE DONE]

Description of Systems

[Summary of systems that will be involved in the initiative; if talking at early stage could just be a list if later in the process could be indicative architecture. Should specify what internal systems are likely to be touched as well as any external agencies interacted with, cloud systems, information transfer / sharing mechanisms. Include a description of the nature of the changes to existing system, if known. JUST INCLUDE WHAT YOU KNOW, YOU DON'T NEED TO HAVE A FULL UNDERSTANDING AT THIS STAGE; JUST NEED TO KNOW ENOUGH TO BE ABLE TO IDENTIFY THE SCOPE OF WORK TO BE DONE]

Security Assessment Requirements

Prior to go-live the following must be completed for this initiative:

☐ No C&A required – no further action required
☐ No C&A required – put into re/certification backlog
☐ C&A required – Risk Assessment
☐ C&A required – Change Certification

C&A Scope:	[IF C&A REQUIRED insert scope summary making clear what **business processes / systems are within scope and what is excluded.** Scope may cover all aspects of an initiative / the end-to-end information flow, or it may be focussed on / limited to only certain parts of this. **Where the scope is limited, make sure it is clear what will be covered and what will not, and why**. Scope may be limited for many reasons, but the main ones will be 1) some components have already been certified and do not need to be reassessed, 2) there are only certain points in the end-to-end flow where there are security risks, or 3) there may be only certain risks that are relevant given the nature of the initiative. **Scope may also be limited to only validation of controls**. This would be the case when 1) a system has been previously certified for pre-defined use cases but specified controls must be validated for every new use (eg controls that must be validated for each new data transfer

	using the Data Exchange), 2) there are clear MSD or government standards that must be met for the system type (eg GCDO control requirements for low risk websites). **If penetration test required, identify that now]** IF NO C&A REQUIRED DELETE THIS ROW
Rationale for "no C&A required":	[IF NO C&A REQUIRED insert justification for why] IF C&A REQUIRED DELETE THIS ROW
System Classification:	Choose an item. [When determining the classification level that a system needs to be certified for consider whether it is possible that information at a higher classification might be generated / received / stored, even if that is not the intent of the system. In particular, consider whether it needs to be classified to RESTRICTED level. While MSD doesn't generally create RESTRICTED information it is possible, particularly in times of national emergency (eg Christchurch Mosque attack, COVID-19 response), that we could, or more likely that we could receive this information and have a need to securely receive and store it electronically.]
Completed by:	
Reviewed by:	Choose an item.
Date:	Click or tap to enter a date.

Privacy Assessment Requirements

Prior to go-live the following must be completed for this initiative:

☐ No C&A Required – no further action required
☐ No C&A Required – provide advice only
☐ C&A Required – Impact / Risk Assessment
☐ C&A Required – Change Certification

C&A Scope:	[IF C&A REQUIRED insert scope summary making clear what **business processes are within scope and what is excluded.** Scope may cover all aspects of an initiative / the end-to-end information flow, or it may be focussed on / limited to only certain parts of this. **Where the scope is limited, make sure it is clear what will be covered and what will not, and why.** Scope may be limited for many reasons, but the main ones will be 1) some components have already been certified and do not need to be reassessed, 2) there are only certain points in the end-to-end flow where there are privacy risks, 3) there may be only certain privacy principles that are relevant given the nature of the initiative, 4) the initiative sits alongside a business as usual process where some / many of the IPPs are already dealt with and the initiative doesn't change these; the assessment will focus only on what is changing. **Scope may also be limited to only validation of controls.** For example, this would be the case when a system or process has been previously certified for pre-defined use cases but specified controls must be validated for every new use (eg controls that must be validated for each new data transfer using the Data Exchange)] IF NO C&A REQUIRED DELETE THIS ROW
Rationale for "no C&A required":	[IF NO C&A REQUIRED insert justification for why] IF C&A REQUIRED DELETE THIS ROW
Completed by:	
Reviewed by:	Choose an item.
Date:	Click or tap to enter a date.

Human Rights & Ethics Assessment Requirements

Prior to go-live the following must be completed for this initiative:

☐ C&A Not Required – no further action required
☐ C&A Not Required – provide advice only
☐ C&A Required – Impact / Risk Assessment
☐ C&A Required – Change Certification

C&A Scope:	[Insert scope summary making clear what is within the scope and what is excluded and why]
Rationale for "no C&A required":	[IF NO C&A REQUIRED insert justification for why] IF C&A REQUIRED DELETE THIS ROW
Completed by:	
Reviewed by:	Choose an item.
Date:	Click or tap to enter a date.

Information Sharing Requirements

Prior to go-live the following must be completed for this initiative:

☐ No information sharing
☐ No current sharing agreement exists – new agreement required as follows:
- ☐ New AISA
- ☐ New MOU
- ☐ New Letter of Agreement

☐ Existing sharing agreement exists – updates required as follows:
- ☐ Updates to existing Approved Information Sharing Agreement (AISA)
- ☐ New Memorandum of Understanding (MOU) under existing AISA
- ☐ Updates to existing MOU
- ☐ Updates to existing Letter of Agreement
- ☐ Updates to existing Information Matching Agreement

Scope:	[outline the scope of the MOU / AISA etc if it is able to be identified at this stage] IF NO INFORMATION SHARING DELETE THIS ROW
Completed by:	
Reviewed by:	Choose an item.
Date:	Click or tap to enter a date.

Security, Privacy, Human Rights & Ethics Assessment

[INSERT NAME]

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Report Data

Name of Initiative

Business Owner

Choose an item.

Stakeholder(s)

<Name, Title>

Objective ID

Reference Documents

- [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 ie is it medical information, aggregated data, identifiable information about singular individuals, identifiable information about groups of individuals, information about family / sexual violence, etc 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

[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.

[**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.]

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.

[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]

[Scope may be limited for a range of reasons, but the main ones will be 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.

[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.]

[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 some / many of the IPPs are already dealt with and the initiative doesn't change these; the assessment will focus only on what is changing. If "other" is selected note below the rationale and specific limitation.]

Human Rights & Ethics - 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 some / many of the IPPs are already dealt with and the initiative doesn't change these; the assessment will focus only on what is changing. If "other" is selected note below the rationale and specific limitation.]

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 don't 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.]

Compliance to Standards

Standard	**Compliant**	**Comment** *(Comments and link to remediation plan required where not compliant)*
Encryption Standard	Yes/No	

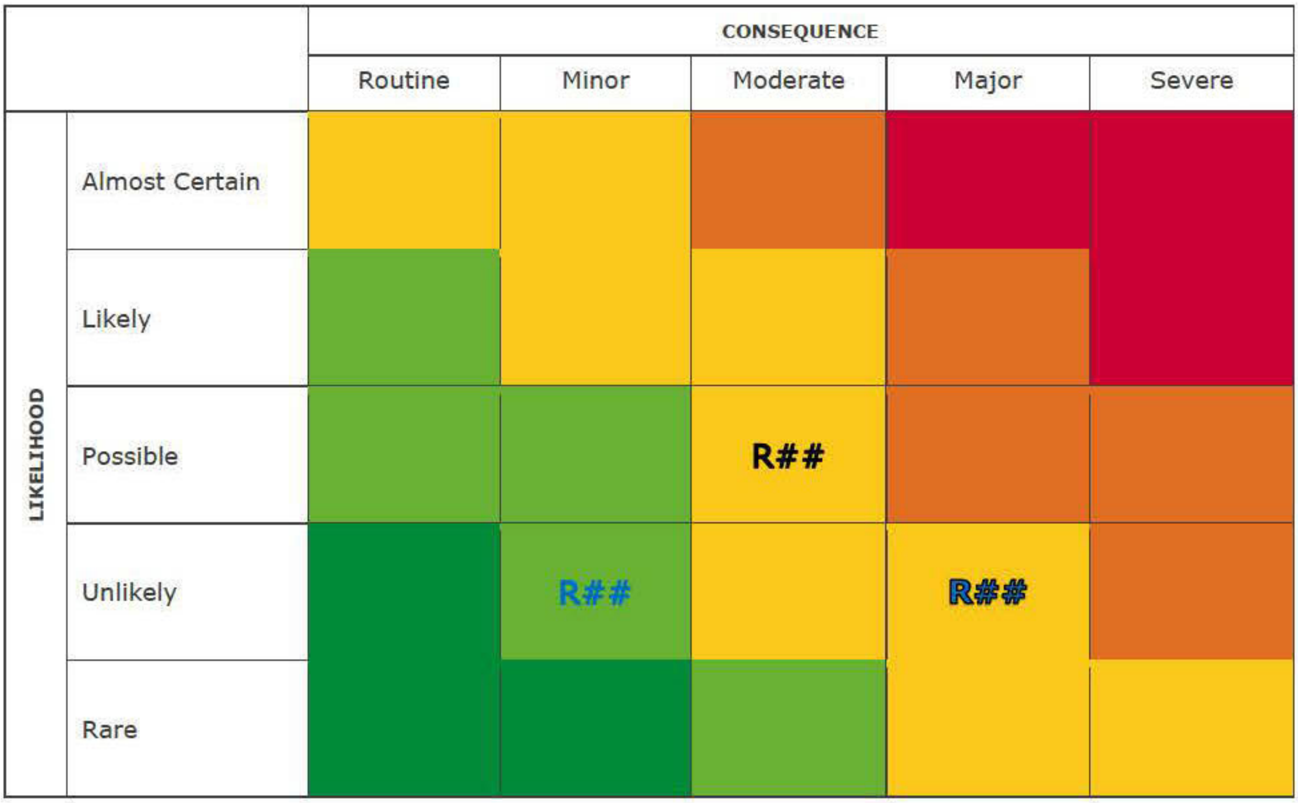
Key Management Standard	Yes/No
Data Jurisdiction Standard	Yes/No
Authentication Standard	Yes/No
Service Security Baseline	Yes/No
Patch Management Standard	Yes/No
Vulnerability Management Standard	Yes/No
Information Classification	Yes/No
Password Standard	Yes/No
Remote Access Standard	Yes/No
Automated Decision-Making Standard	Yes/No
Third-party Provider Information Assurance Standard	Yes/No

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##

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]

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

☐ Certified
☐ Qualified Certification
☐ Not Certified

Comments

[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]

[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]

Hannah Morgan, Chief Information Security Officer / Chief Privacy Officer Date

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.

Accreditation

☐ Accredited
☐ Qualified Accreditation
☐ Not Accredited

Comments

Choose an item. Date

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.

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	**Risk Title** [Something Happens… for example an incident or a natural disaster or data leak happens – more examples can be found in the Risk Catalogue (A12035849)] [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)] KEEP EACH LINE TO NO MORE THAN ONE PAGE **This may result in:** - Choose an item. - Choose an item. **Example Scenario(s): <This could be an actual example scenario(s) that could potentially happen if this risk is not mitigated>** - … - … **Affects:** ☐ Confidentiality, ☐ Integrity, ☐ Availability	Risk (consequence / likelihood) [colour cell according to risk rating]	[Insert list of controls – Please refer to the Control Catalogue to choose the appropriate controls best suited for this risk. 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 *Current Residual Risk* should be assessed on the basis of, controls that are assessed as (per Appendix 2): - Effective - Not Yet Assessed (evidence doesn't 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: - 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	**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] **Affects:** IPP1, IPP2, IPP3, IPP4, IPP5, IPP6, IPP7, IPP8, IPP9, IPP10, IPP11, IPP12 [delete all those not relevant]	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; don't just list everything they're 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 *Current Residual Risk* should be assessed on the basis of, controls that are assessed as (per Appendix 2): ▸ Effective ▸ Not Yet Assessed (evidence doesn't 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: ▸ The consequence is reduced by… ▸ The likelihood is reduced by…]

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; don't just list everything they're 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 *Current Residual Risk* should be assessed on the basis of, controls that are assessed as (per Appendix 2): - Effective - Not Yet Assessed (evidence doesn't 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: - The consequence is reduced by… - The likelihood is reduced by…]

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.

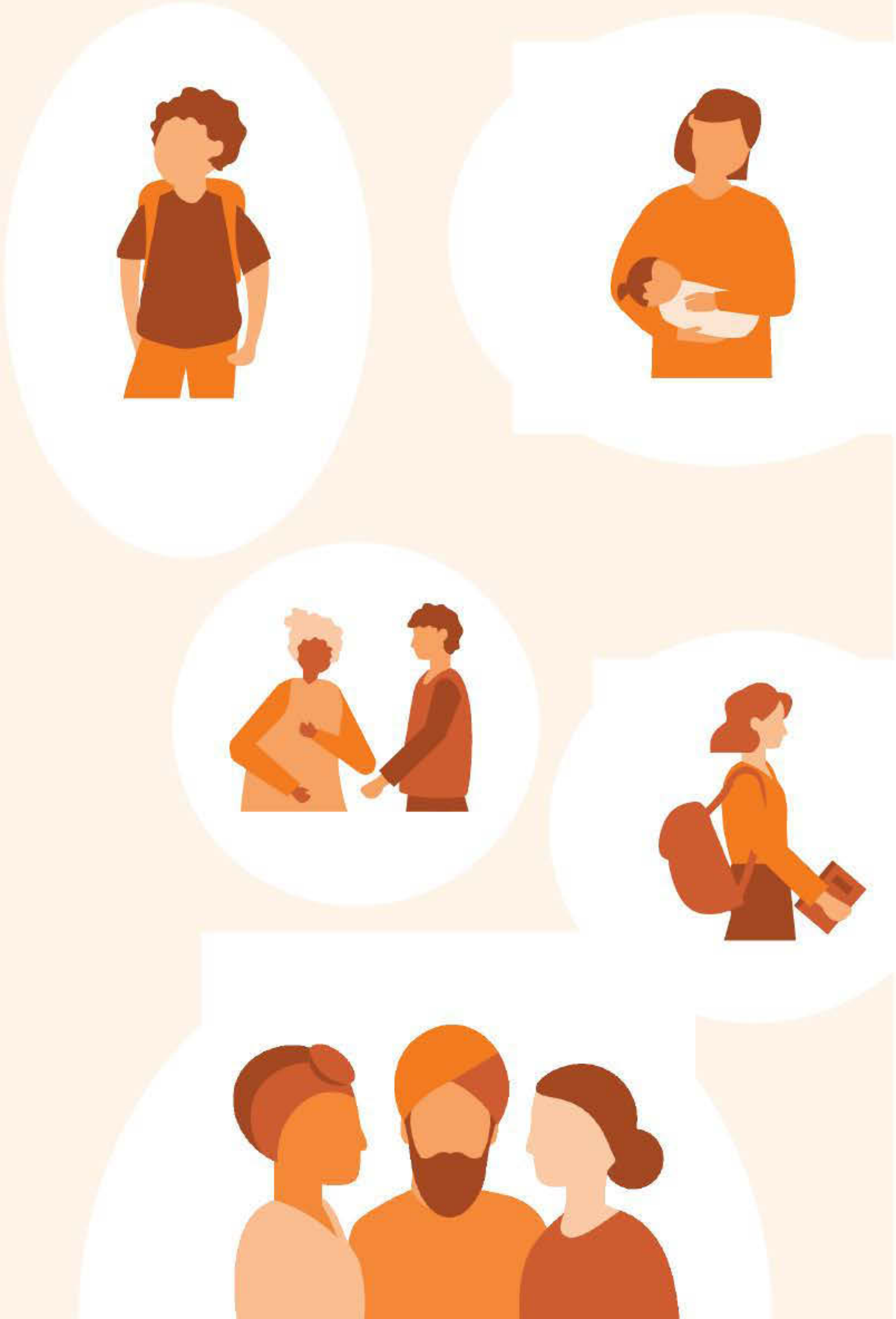
#	Control Description	Control Validation Activities Completed	Control Effectiveness	Agreed Remediation Activity (where control ineffective / partially effective)
C01	**Title [should match risk table, highlight title green if key control]** [include description of control] **Control Owner:** [Insert name, 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 won't be remediated and what the Ministry standard is in this area. 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]

The Data Protection & Use Policy

An introduction...

In short…

- Developed by the social sector for the social sector
- on the collection or use of data or information, *from or about,* service users
- recommendations go beyond the law, and are clear when they do so, and why
- provides guidance how to do this in the most respectful, transparent and trustworthy way
- focuses on relationships, values and behaviours more than rules
- A ‘good practice guide’, in a way that makes sense in the context.



The Power of Data

The superpower is used in all sorts of situations like:

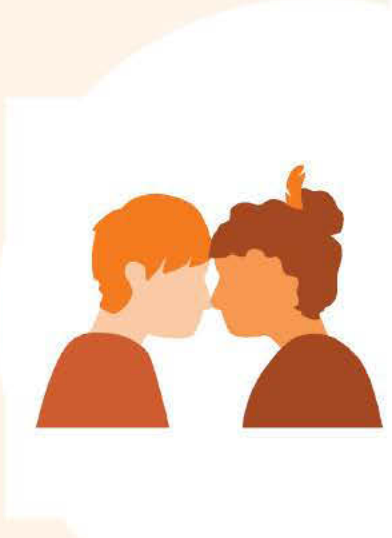
- When service users are **asked to fill out a form about themselves**, that information or data is recorded and may be used to make decisions or provide them with support
- When decision makers are thinking about what data and information service users should be asked, for example to:
    - decide if they are **eligible** for a service
    - learn how **helpful** a service or programme is
    - help make decisions about how much **money** a service needs, or if there should be **different types** of service or programmes for people
    - help **understand** what situations look like for service users and communities
- When data or information from, or about, service users is being **looked at, made sense of, or used in any way** (like the above examples) - even if the person using it doesn't know the individuals who the information is about.

It all starts with "why"

Why should I learn about the Policy or think about it in my work?

Because the social sector is about **He tāngata**

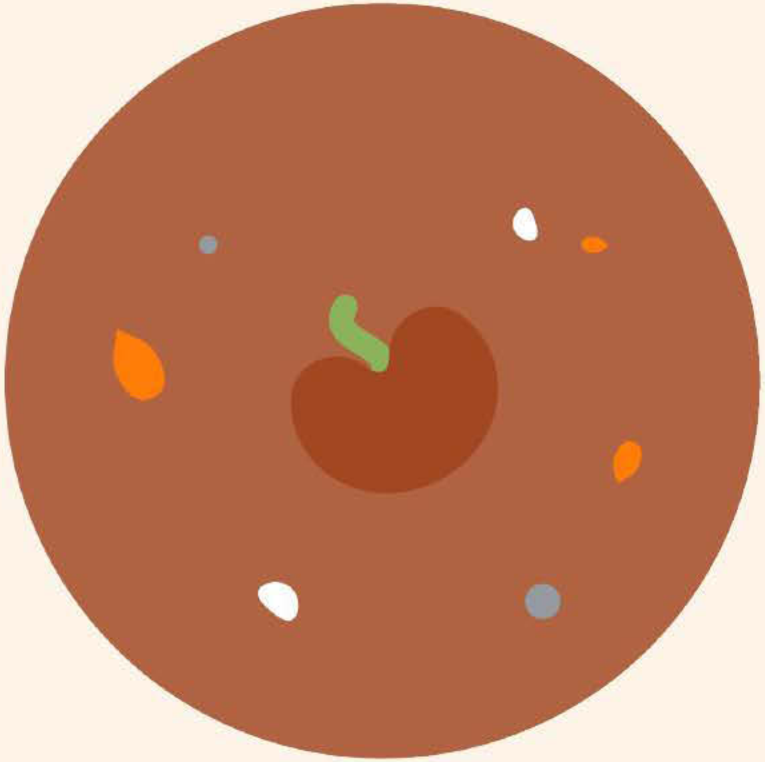
Because data and information is **powerful**



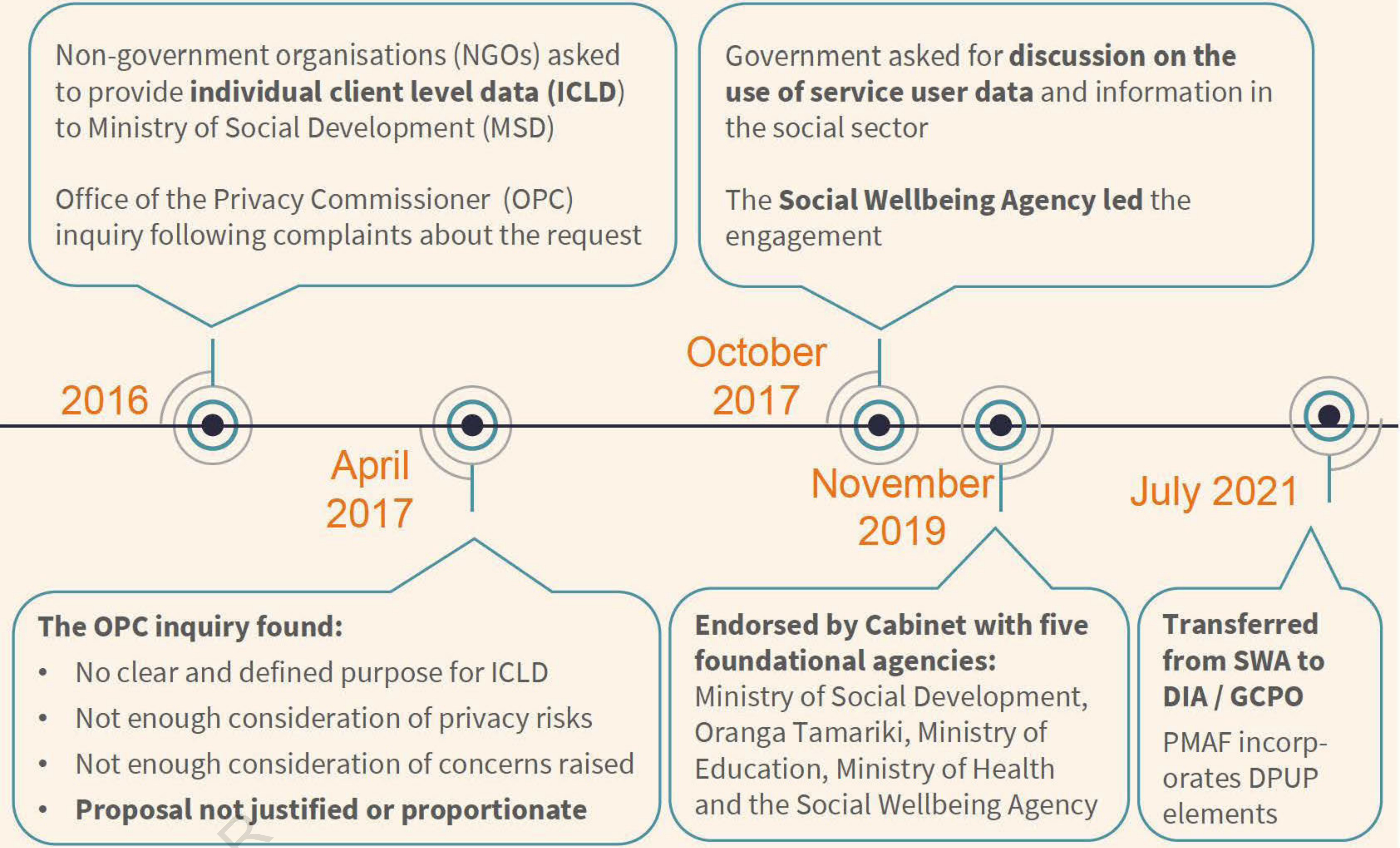
The **Policy** will help you…

- use data and information in the most **respectful**, **transparent** and **trustworthy** way
- use it to **grow the knowledge** of the sector about how best to support New Zealanders wellbeing
- build **trust with service users** in how you care for their information.

The Journey



The Journey



2016

Non-government organisations (NGOs) asked to provide **individual client level data (ICLD)** to Ministry of Social Development (MSD)

Office of the Privacy Commissioner (OPC) inquiry following complaints about the request

April 2017

The OPC inquiry found:

- No clear and defined purpose for ICLD
- Not enough consideration of privacy risks
- Not enough consideration of concerns raised
- **Proposal not justified or proportionate**

October 2017

Government asked for **discussion on the use of service user data** and information in the social sector

The **Social Wellbeing Agency led** the engagement

November 2019

Endorsed by Cabinet with five foundational agencies: Ministry of Social Development, Oranga Tamariki, Ministry of Education, Ministry of Health and the Social Wellbeing Agency

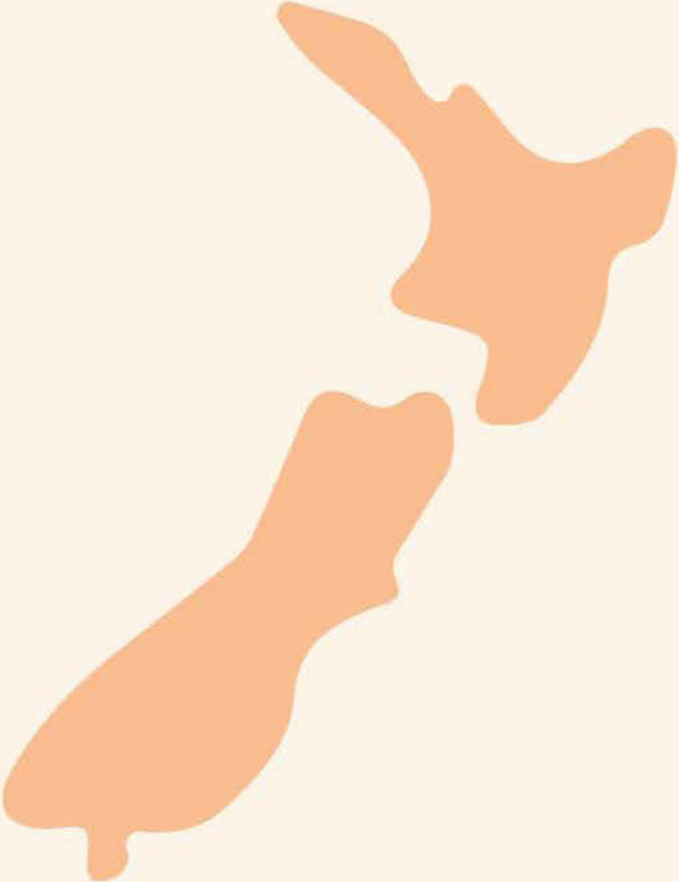
July 2021

Transferred from SWA to DIA / GCPO

PMAF incorporates DPUP elements

Engagement: Your voice, your data, your say

Between May and September 2018, the Social Wellbeing Agency asked New Zealanders for their thoughts about the Investing for Social Wellbeing Approach and **what's reasonable and what's not** when using people's information.



27
Locations

83
Hui

1047
People

801
Online survey responses

What would you say?

These are some of the questions asked during the engagement ....

When we think about using people’s information, what’s reasonable and what’s not?

How can organisations make it easy for people to understand what happens with their information?

What principles should guide our thinking and our behaviour on this topic?

What would you say?

What people said

"People are not numbers, stories create authentic data."

"Counsellors have huge files but won't share that with me and it's all about me!"

"Nothing about us without us."

"Honestly of purpose is our tikanga and kawa."

"How do we best kaitiaki the pūrākau that have been so trustingly shared?" (How do we care for the stories?)

"We over collect because we haven't defined what the purpose is."

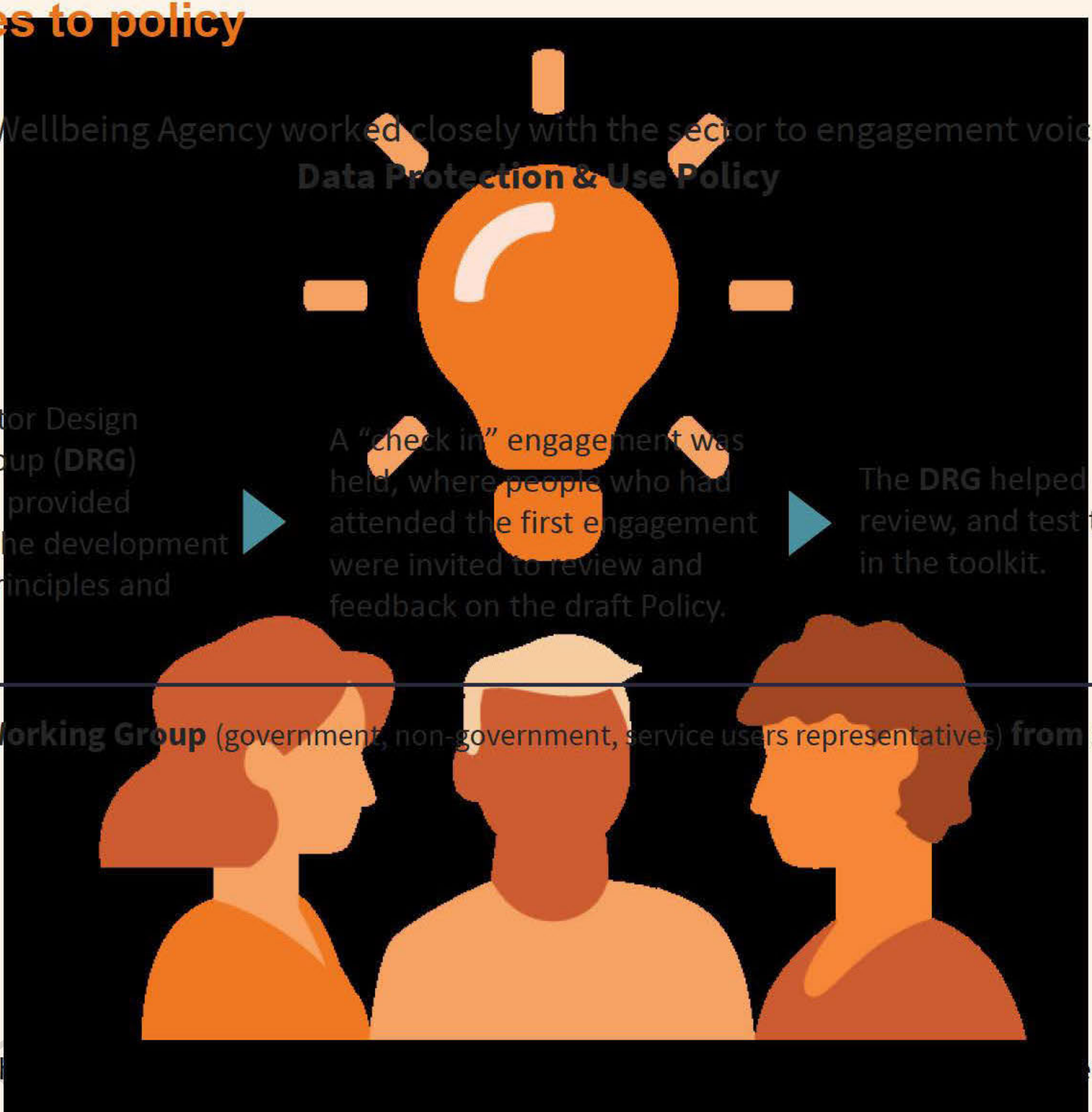
"It has to be about everyone, not just the government"

"Before you democratise data you've got to decolonise it."

"If the community holds the data, whānau can make better decisions about their lives."

"Be crystal clear about the why. Why is this information needed, and how it will be used for service provision."

From voices to policy



The Social Wellbeing Agency worked closely with the sector to engagement voices into the **Data Protection & Use Policy**

The cross-sector Design Reference Group (**DRG**) reviewed and provided feedback on the development of the draft Principles and Guidelines.

A “check in” engagement was held, where people who had attended the first engagement were invited to review and feedback on the draft Policy.

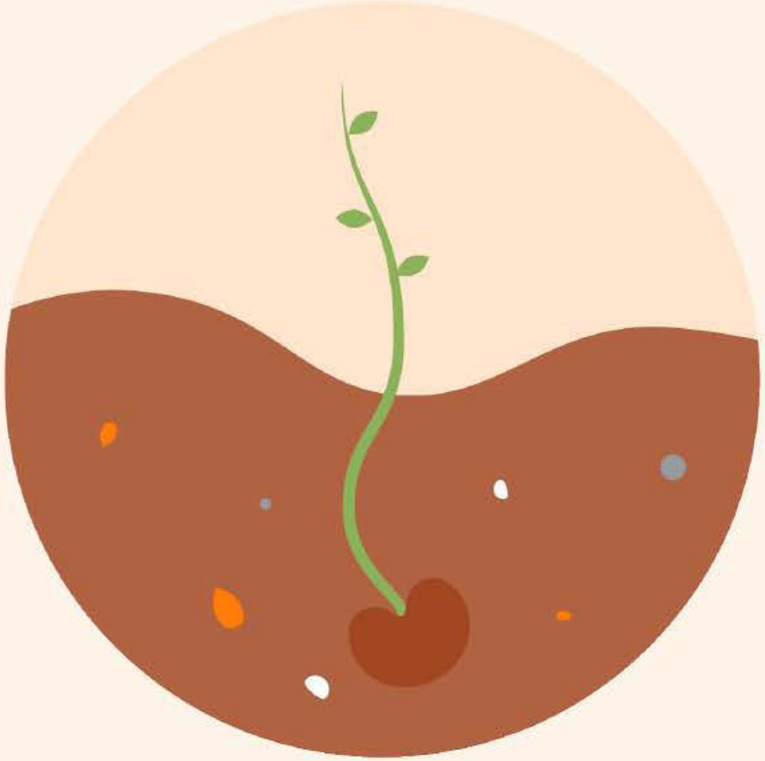
The **DRG** helped design, review, and test the resources in the toolkit.

Ministerial Working Group (government, non-government, service users representatives) **from start to finish**

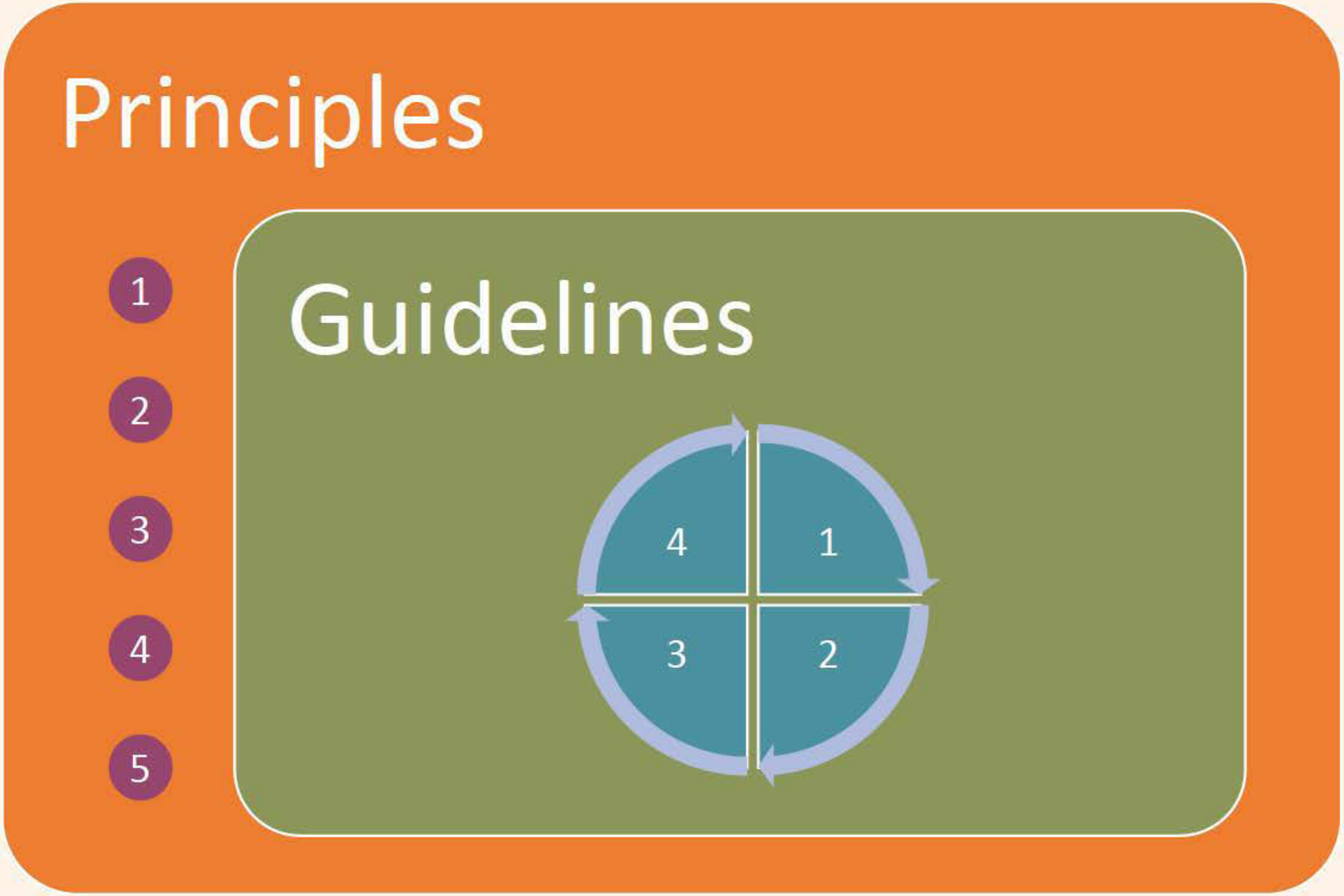
Note: Th

ncies.

The Policy



The structure



The Five Principles

The **Policy** and the **Principles** are more about relationships than rules

Because everything we do in the social sector is about **He tāngata** – the people

He tāngata — Focus on improving people's lives – individuals, children and young people, whānau, iwi and communities.

Manaakitanga — Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.

Mana whakahaere — Empower people by giving them choice and enabling their access to, and use of, their data and information.

Kaitiakitanga — Act as a steward (a Kaitiaki) in a way that is understood and trusted by New Zealanders.

Mahitahitanga — Work as equals to create and share valuable knowledge.

The Four Guidelines

Purpose Matters

Be clear about the purpose of collecting or using people's information. Collect only what is needed.

Consider how using people's information might affect their wellbeing and their trust in those using it.

Transparency and Choice

Be transparent and help people understand why their information is needed and what happens with it.

As much as possible support their choices about what they want to share and how they want it used.

Access to Information

Be proactive about supporting people to understand what information is held about them. Their rights to access it and ask for corrections to be made.

Look for ways to make this easy and safe for service users.

Sharing Value

Work together, collaborate to make sure the best information is used in the most respectful and helpful way.

Share insights across the sector to help grow knowledge and support wellbeing.

The Toolkit

To access all the resources in the toolkit go to **dpup.swa.govt.nz**

What does this mean for MSD as a Foundation Agency?

- The Ministry is committed to lifting trust and confidence in its use of data and information including looking at how we can be more transparent about our data and information collection and use, and identifying opportunities to provide choice
- To support this, the Information Group, as Custodian of DPUP for MSD, has incorporated DPUP into the Privacy, Human Rights and Ethics framework (the PHRaE).

What does this mean for [our/your Portfolio/team]?

- [IF there are known initiatives write them here, OR
- propose this as a question about how portfolios, teams and individuals could influence or directly help to lift trust and confidence in how the Ministry, Portfolio, team or individual; AND
- ask what the challenges in doing so would be]

The Quiz

1. Who is the Policy primarily for?

A. **Government agencies**

B. **Any kind of NGO or charity in New Zealand**

C. **The whole social sector including government agencies, Non-Government Organisations (NGOs) and other service providers**

D. **Any business or organisation that collects information about people**

1. Who is the Policy primarily for?

The correct answer is C

“The whole social sector including government agencies, Non-Government Organisations (NGOs) and other service providers.”

Note*: While DPUP was primarily created for the social sector, certain elements now incorporated into the Privacy Maturity Assessment Framework (PMAF) making applicable for ALL government agencies.*

2. What are the Data Protection & Use Principles?

A. He tāngata, Manaakitanga, Mana whakahaere, Kaitiakitanga and Mahitahitanga

B. Partnership, Participation and Protection

C. Purpose Matters, Transparency & Choice, Access to Information and Sharing Value

D. Rangatiratanga (Authority), Whakapapa (Relationships), Whanaungatanga (Obligations), Kotahitanga (Collective Benefit), Manaakitanga (Reciprocity) and Kaitiakitanga (Guardianship)

2. What are the Data Protection & Use Policy Principles?

The correct answer is A:

The **summary** of each principle is shown below.
The **full** versions can be found https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/data-protection-and-use-policy-dpup/read-the-dpup-principles/

He tāngata	Focus on improving people's lives – individuals, children and young people, whānau, iwi and communities
Manaakitanga	Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information
Mana whakahaere	Empower people by giving them choice and enabling their access to, and use of, their data and information
Kaitiakitanga	Act as a steward (a Kaitiaki) in a way that is understood and trusted by New Zealanders
Mahitahitanga	Work as equals to create and share valuable knowledge

3. Which statement best summarises the “Purpose Matters” Guideline?

A. Being clear about why you need data means it’s easier to collect what you need right now, as well as things that you might need at some point in the future.

B. Be clear about purpose from the start to make sure data or information collection or use is based on a clear understanding of why it is needed, and ensures that people’s information is used in a way that improves wellbeing and builds trust.

3. Which statement best summarises the “Purpose Matters” Guideline?

The correct answer is B

“Be clear about purpose from the start to make sure data or information collection or use is based on a clear understanding of why it is needed, and to ensure that people’s information is used in a way that improves wellbeing and builds trust.”

The **Purpose Matters** guideline encourages broader thinking, focused on the social sector and the relationships between New Zealander’s who access social services, the providers, and funders (usually government).

Being clear about purpose and involving others in its development is a foundation to having the most relevant, useful data or information and collecting and using it in a respectful, trusted and transparent way.

4. Which statement best summarises the “Transparency & Choice” Guideline?

A. **Aim for a “no surprises” approach – service users shouldn’t be surprised about what information is held about them or how it’s used.**

Look for ways to provide as many choices as possible – around what information people need to provide, how it’s recorded, who sees it, how it’s shared or used.

B. **As long as there is no way to identify someone when their information or data is used, then they don’t need to know what it’s been used for.**

If people want to engage with social services then they aren’t able to have any choices about how or why their data or information is collected or used, or who gets to have it or see it.

4. Which statement best summarises the “Transparency & Choice” Guideline?

The correct answer is A

*“Aim for a ‘**no surprises**’ approach – service users shouldn’t be surprised about what information is held about them or how it’s used.*

Look for ways to provide as many choices as possible – around what information people need to provide, how it’s recorded, who sees it, how it’s shared or used.”

5. Which statement best summarises the “Access to Information” Guideline?

A. **Under the Privacy Act people have the right to access, and ask for corrections to, their personal information.**

The Access to Information guideline is about **Mana Whakahaere** and being proactive around these rights. Explain these rights in a way people will understand, make it safe and easy to use them, or look for ways to offer access without service users even having to ask.

B. **Under the Privacy Act people have the right to access, and ask for corrections of their personal information.**

Access to information is about having processes in place to respond to peoples written requests to access their information.

5. Which statement best summarises the “Access to Information” Guideline?

The correct answer is A

“Under the Privacy Act people have the right to access, and ask for corrections of their personal information.

*The Access to Information guideline is about **Mana Whakahaere** and being proactive around these rights. Explain these rights in a way people will understand, make it safe and easy to use them, or look for ways to offer access without service users even having to ask.”*

IMPORTANT TO KNOW: There is no legal requirement for people to put a request in writing for their information.

6. Which statement best summarises the “Sharing Value” Guideline?

A. **All data and information across the social sector should be open and accessible by anyone who wants it.**

Sharing Value means that at the end of any work with data and information we let people know what we learned.

B. **To make the most of the opportunities that comes from data and information. Share the results, insights, analysis or protected data with those who have a legitimate interest or use for it.**

Sharing Value is also about collaborating and having strong partnerships when it comes to making decisions about the collection or use of people’s data or information.

Involve others with an interest in your work, including service users if possible, from the beginning.

6. Which statement best summarises the “Sharing Value” Guideline?

The correct answer is B

To make the most of the opportunities that comes from data and information. Share the results, insights, analysis or protected data with those who have a legitimate interest or use for it.

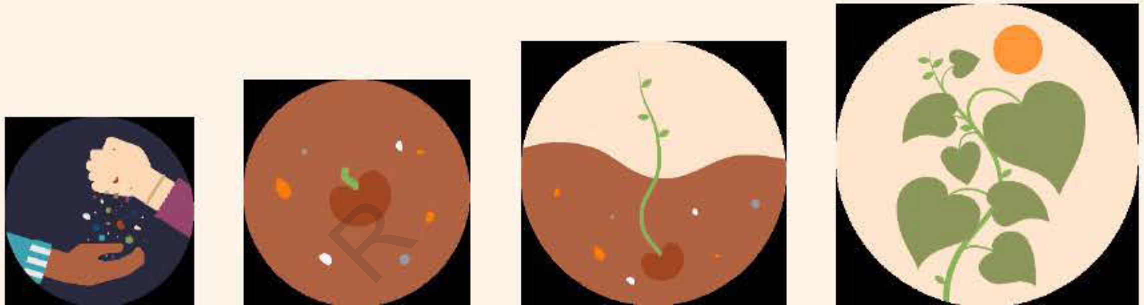
Sharing Value *is also about collaborating and having strong partnerships when it comes to making decisions about the collection or use of people’s data or information.*

Involve others with an interest in your work, including service users if possible, from the beginning.

Wrap up

dpup.swa.govt.nz

for more on the Data Protection & Use Policy, Principles, Guidelines and toolkit



Privacy, Human Rights & Ethics Framework

Guidance: Key considerations

Purpose

To outline common areas that need to be understood or considered when working through the Ministry's Privacy, Human Rights and Ethics (the PHRaE) framework.

Overview

The PHRaE helps ensure that we act responsibly when we use personal information to achieve better outcomes for our clients.

The PHRaE focuses on legislative and compliance considerations for the collection, use or disclosure of personal information. It also incorporates guidance from **Te Tiriti o Waitangi/The Treaty of Waitangi**, the **Data Protection and Use Policy** and the **Algorithm Charter for Aotearoa New Zealand**.

The PHRaE process is intended to identify the challenges to privacy, human rights, and ethical interests posed by a proposed use of personal information and to help Ministry staff respond appropriately.

Key considerations

The following areas should be clearly understood before you start discussing a proposal to collect, use, store or distribute personal information in any situation.

Purpose	***"Our purpose is Manaaki tangata, Manaaki whānau – We help New Zealanders to be safe, strong and independent."*** *We help New Zealanders by fulfilling a broad range of responsibilities and functions, including:* • *providing employment, income support and superannuation services* • *designing and delivering community services in conjunction with others* • *allocating funding to community service providers* • *providing student allowances and loans* • *providing public housing assistance and services* • *being the primary provider of social policy and advice to Government* • *monitoring three Crown entities and providing advice to the responsible Minister*

- *ensuring the legislation we administer is effective and fit-for-purpose*
- *working with other agencies and the wider social sector to support Government priorities and*
- *improve the wellbeing of all New Zealanders.*

There must be a clear link between the purpose information is being collected or used for and the Ministry's legislative purpose. However, consideration of sensitivities and possible adverse consequences should also be made, even where collection is lawful. This is covered under the more detailed PHRaE guidance materials.

If personal information isn't necessary to achieve the objectives required, we shouldn't collect, use, store or share it.

Personal information

There are many types of personal information, including:

- names, addresses, phone numbers and email addresses
- unique identifiers
- SWN, IRD, and NHI numbers
- photos, videos or audio recordings
- financial or medical records
- ethnicity, and iwi and hapū affiliation
- religious details
- handwritten notes, opinions and allegations
- records of our interactions with a client.

Even if the information does not appear to be personal, you should consider if it might be able to be linked to an individual when combined with other available information.

For example, a description of a person as someone 'who had a hip operation at a named DHB' will be personal information if someone could use that information, together with information about surgical patients and conditions at the DHB, to work out who the person is.

Other factors

Contextual, environmental, or cultural factors should also be considered when or how people are asked for their information. This could include addressing language barriers, low literacy or comprehension levels, a disability, environmental or cultural preferences, for example, a Kaupapa Māori approach.

These factors do not mean we should not collect, use, or distribute information. Instead it highlights our responsibility to ensure there is a **meaningful purpose** for doing so that could be explained to the person whose information it is, and in a way that they would understand and find reasonably necessary.

Te Tiriti o Waitangi

The Ministry is committed to Te Tiriti o Waitangi / the Treaty of Waitangi through authentic consultation and engagement processes. When services are likely to have particular significance for Māori, involving iwi or Māori in the proposed use of their information is especially important. Funding and timelines for a proposal should factor this in unless there is a compelling reason not to.

See: Te Pātaka Korero a Rua to seek further guidance.

Māori Data Governance

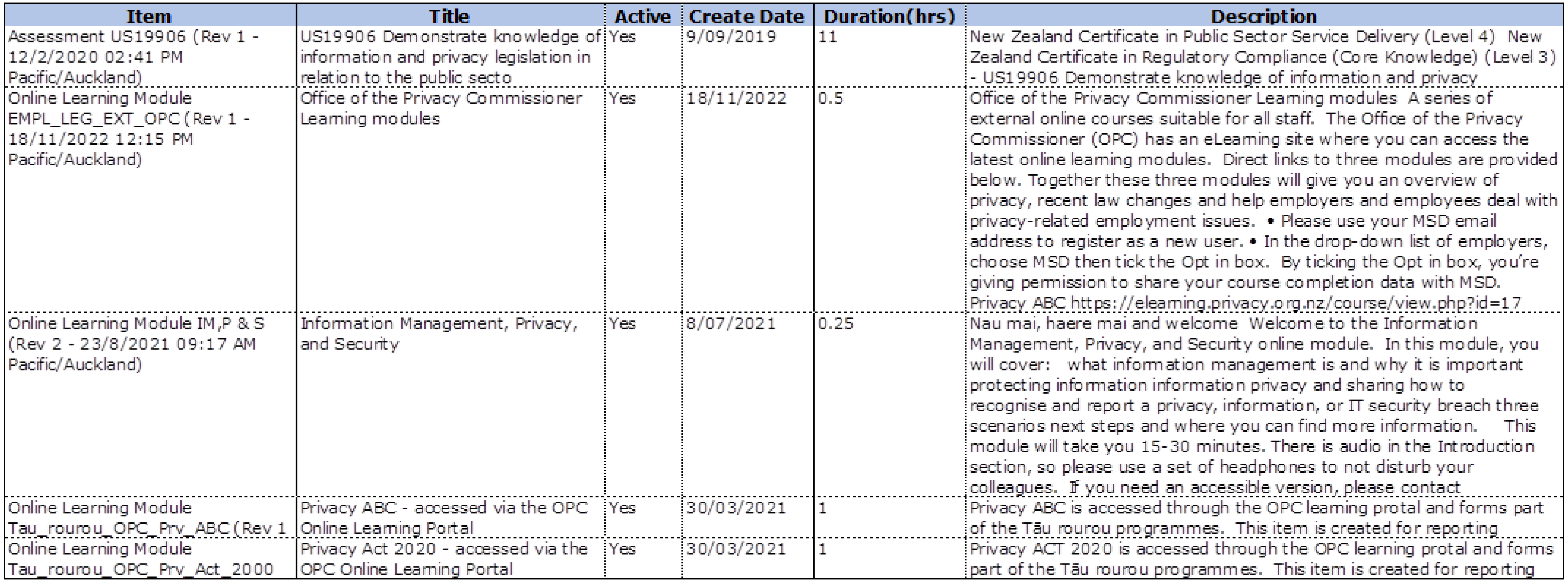
There is currently no confirmed direction for the Public Sector or the Ministry on Māori Data Governance. Until there is clear guidance, no advice should be provided in this area. You can talk to a senior adviser or your manager if this subject is raised by your Portfolio.

Appendix Two

Staff who undertake the following qualifications are also required to complete US19906 Demonstrate knowledge of information and privacy legislation in relation to the public sector:

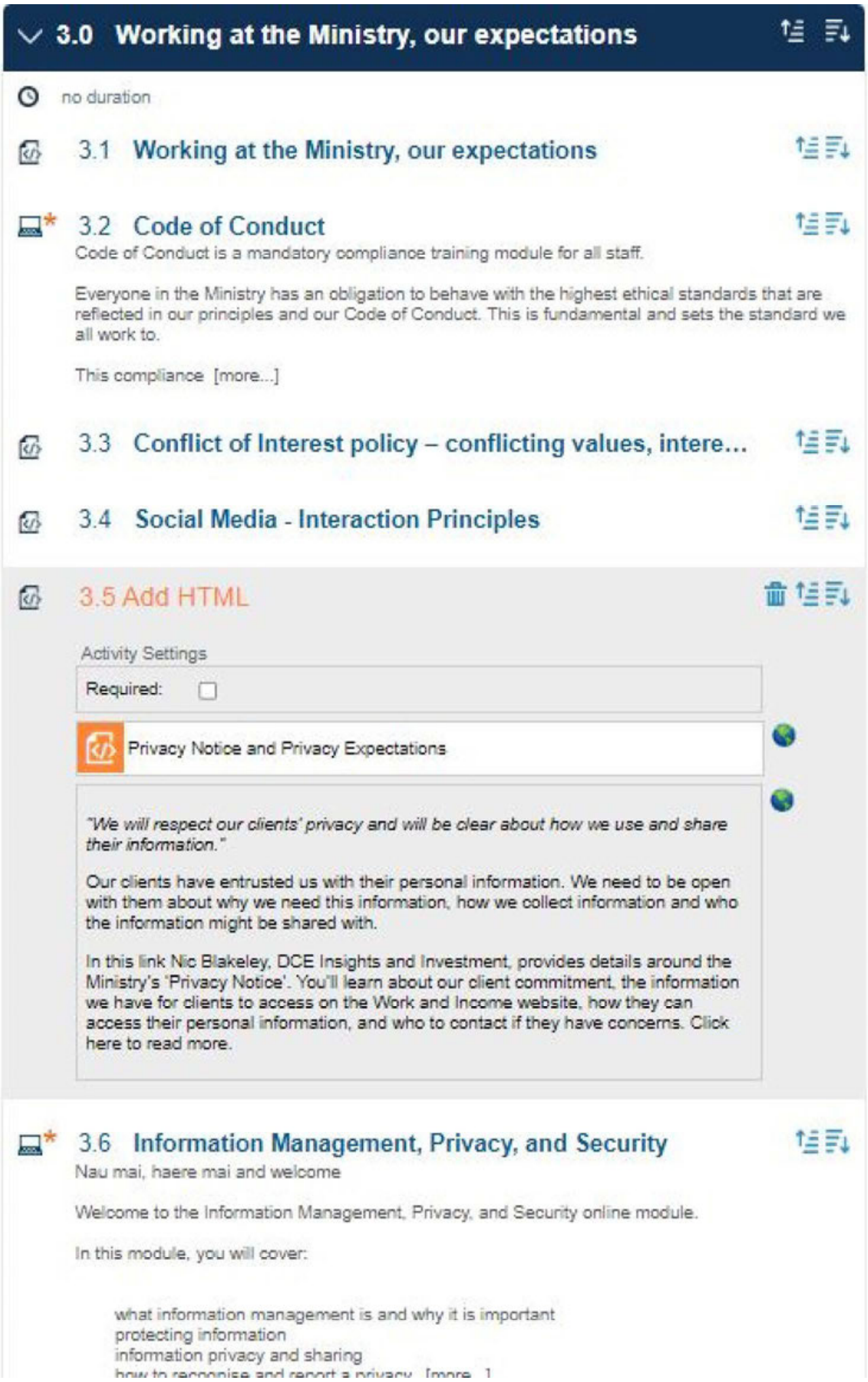
- NZ Certificate in Public Sector Service Delivery (Level 4)
- NZ Zealand Certificate Regulatory Compliance (Core Knowledge) (Level 3)

Course Overviews:



Item	Title	Active	Create Date	Duration(hrs)	Description
Assessment US19906 (Rev 1 - 12/2/2020 02:41 PM Pacific/Auckland)	US19906 Demonstrate knowledge of information and privacy legislation in relation to the public secto	Yes	9/09/2019	11	New Zealand Certificate in Public Sector Service Delivery (Level 4) New Zealand Certificate in Regulatory Compliance (Core Knowledge) (Level 3) - US19906 Demonstrate knowledge of information and privacy
Online Learning Module EMPL_LEG_EXT_OPC (Rev 1 - 18/11/2022 12:15 PM Pacific/Auckland)	Office of the Privacy Commissioner Learning modules	Yes	18/11/2022	0.5	Office of the Privacy Commissioner Learning modules A series of external online courses suitable for all staff. The Office of the Privacy Commissioner (OPC) has an eLearning site where you can access the latest online learning modules. Direct links to three modules are provided below. Together these three modules will give you an overview of privacy, recent law changes and help employers and employees deal with privacy-related employment issues. • Please use your MSD email address to register as a new user. • In the drop-down list of employers, choose MSD then tick the Opt in box. By ticking the Opt in box, you're giving permission to share your course completion data with MSD. Privacy ABC https://elearning.privacy.org.nz/course/view.php?id=17
Online Learning Module IM,P & S (Rev 2 - 23/8/2021 09:17 AM Pacific/Auckland)	Information Management, Privacy, and Security	Yes	8/07/2021	0.25	Nau mai, haere mai and welcome Welcome to the Information Management, Privacy, and Security online module. In this module, you will cover: what information management is and why it is important protecting information information privacy and sharing how to recognise and report a privacy, information, or IT security breach three scenarios next steps and where you can find more information. This module will take you 15-30 minutes. There is audio in the Introduction section, so please use a set of headphones to not disturb your colleagues. If you need an accessible version, please contact
Online Learning Module Tau_rourou_OPC_Prv_ABC (Rev 1	Privacy ABC - accessed via the OPC Online Learning Portal	Yes	30/03/2021	1	Privacy ABC is accessed through the OPC learning protal and forms part of the Tāu rourou programmes. This item is created for reporting
Online Learning Module Tau_rourou_OPC_Prv_Act_2000	Privacy Act 2020 - accessed via the OPC Online Learning Portal	Yes	30/03/2021	1	Privacy ACT 2020 is accessed through the OPC learning protal and forms part of the Tāu rourou programmes. This item is created for reporting

Employee Induction Module Section 3 - Ministry expectations showing 3.5 privacy expectations and 3.6 mandatory module including assessment on Information Management, Privacy and Security.



3.0 Working at the Ministry, our expectations

no duration

3.1 Working at the Ministry, our expectations

3.2 Code of Conduct

Code of Conduct is a mandatory compliance training module for all staff.

Everyone in the Ministry has an obligation to behave with the highest ethical standards that are reflected in our principles and our Code of Conduct. This is fundamental and sets the standard we all work to.

This compliance [more...]

3.3 Conflict of Interest policy – conflicting values, intere...

3.4 Social Media - Interaction Principles

3.5 Add HTML

Activity Settings

Required: □

Privacy Notice and Privacy Expectations

"We will respect our clients' privacy and will be clear about how we use and share their information."

Our clients have entrusted us with their personal information. We need to be open with them about why we need this information, how we collect information and who the information might be shared with.

In this link Nic Blakeley, DCE Insights and Investment, provides details around the Ministry's 'Privacy Notice'. You'll learn about our client commitment, the information we have for clients to access on the Work and Income website, how they can access their personal information, and who to contact if they have concerns. Click here to read more.

3.6 Information Management, Privacy, and Security

Nau mai, haere mai and welcome

Welcome to the Information Management, Privacy, and Security online module.

In this module, you will cover:

what information management is and why it is important
protecting information
information privacy and sharing
how to recognise and report a privacy [more...]

Copy of Code of Conduct referencing Privacy Act 2020 pg 10; Accessing Information and Misuse of Information page 11.

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Code of Conduct

August 2021

Introduction

As public servants each of us has the opportunity to make a positive difference in the lives of New Zealanders through the work we do.

So we can do our work, the taxpayers of New Zealand entrust us with the stewardship of their money and they trust us to protect their personal information. These are big responsibilities. It is important that the way we conduct ourselves reflects the trust New Zealanders place in us.

That's why we have a Code of Conduct. This Code provides you with guidelines on how to go about your work and how to best serve the government of the day. It is important you are familiar with the Code and that you read it regularly. In fact, it is a requirement if you work here.

The Ministry of Social Development (MSD) has a responsibility to you to be a good employer. You have the right to be treated fairly in all aspects of your job.

In return, there are some things MSD expects from you. The Code of Conduct includes clear expectations about behaviour and conduct we cannot and will not tolerate, and the consequences of not meeting these expectations. The Code clearly outlines the consequences of staff fraud, and the deliberate release of information to third parties without proper authorisation.

The Code of Conduct is a guide for you. It won't cover every situation or requirement you experience in your role. If you are ever unsure about what to do, ask for help.

Contents

Introduction **2**

About the Code of Conduct **4**

- Coverage 4
- Standards for Public Servants 4

Zero tolerance **5**

Fair **6**

- Conflicts of interest 6
- Respecting others 7

Impartial **8**

- Political neutrality 8
- Commenting on government policy 9
- Private communications with Ministers or Members of Parliament 9
- Standing as a Member of Parliament 9

Responsible **10**

- Probity 10
- Information and confidentiality 10
- Accessing information 11
- Misuse of information 11

Trustworthy **12**

- Client relationships 12
- Fraud 12
- Prior or pending convictions 13
- Roles requiring National Security Clearance 13
- Gifts and rewards 13
- Staff who are also clients 13
- Exemptions and other considerations 13

Breaches of the Code of Conduct **14**

- Reporting breaches of the Code of Conduct 14
- Privacy breaches 14
- Reporting serious wrongdoing 15
- If you think MSD has not met its obligations under the Code 15

About the Code of Conduct

The Code of Conduct tells you about the way we work. It outlines how we should deal with the people we work alongside and the people we work for, to help make sure we all:

- work with honesty, integrity and respect
- provide the best possible service and advice to the Government, public, stakeholders and clients, and gain their trust and confidence in what we do
- do the best we can do and be the best we can be – every day.

This Code doesn't cover every possible requirement or situation. It gives us a benchmark to work from and gives others a basis from which to judge the way we are working.

We have policies and procedures that give you more detail on the way we work. You should understand and act on the policies and procedures that apply in MSD. You can find these on our intranet (doogle). Meanwhile, read the Code and understand its contents.

Please note, if you don't meet these standards of conduct your behaviour may result in disciplinary action which could include termination of employment.

It is important you fully understand the Code. If you have questions about parts of the Code and how they apply to you in your role, or you are uncertain as to what some of the information means, ask your manager to explain.

Coverage

The Code applies to anyone who works for us, including:

- employees
- contractors
- consultants
- volunteers at MSD.

Whether you are a permanent staff member, are here temporarily or casually, or are a full-time or part-time worker, the Code applies to you.

The Code is part of your employment terms and conditions. It should be read alongside your employment agreement or contract, our policies and procedures, and the Public Service Standards of Integrity and Conduct.

Standards for Public Servants

The Public Service Commissioner has issued the Public Service Standards of Integrity and Conduct. This document sets out the minimum standards of behaviour expected of public servants and is issued under section 17 of the Public Service Act 2020.

The standards say we must be:

- fair
- impartial
- responsible
- trustworthy.

You can find them in more detail at **https://www.publicservice.govt.nz/resources/code**.

The following pages outline what these standards mean for us as part of MSD, and what policies and procedures help us to comply with them.

Zero tolerance

All public servants are expected to uphold general standards of behaviour which are outlined by the Public Service Commission in the Standards of Integrity and Conduct for the Public Service. In MSD, there are other standards over and above these in some areas because of the work we do.

The Ministry of Social Development is responsible for paying benefits and for prosecuting those who defraud the benefit system. Our clients are required to provide us with highly sensitive, personal information to get what they need, or for our business reasons. This means that in these particular areas the standards we apply to ourselves must be higher than those we expect of others.

For example, it is unacceptable under any circumstances for an MSD staff member to:

- steal from the benefit system or MSD
- interfere with or in any way abuse a child or young person that MSD has a professional relationship with
- sell client information
- deliberately share client details or circumstances with any unauthorised person.

Where a staff member does any of these things, the staff member will be dismissed and the matter may be referred to police. In addition to any penalty the Court might impose, all money fraudulently obtained will have to be repaid in full.

Specific applications of MSD's staff fraud and misuse of information zero tolerance policy are in the following pages. You can find other information in relevant MSD policies on our intranet (doogle).

Fair

We must:

- treat everyone fairly and with respect
- be professional and responsive
- work to make government services accessible and effective
- strive to make a difference to the wellbeing of New Zealand and all its people.

Public Service Commission Standards of Integrity and Conduct: Fair
https://www.publicservice.govt.nz/resources/code/?e200=1516-fair

Conflicts of interest

At MSD we need to make sure we are always fair in the way we deal with people, no matter who they are, what their backgrounds are or what their needs are.

We must avoid any appearance or suggestion of preferential treatment or favouritism towards any individual or organisation which we or you have an interest in.

Because we live and work in our communities, it is sometimes hard to avoid conflicts of interest, whether real or perceived. That makes it even more important that conflicts of interest are identified, avoided when they can be, and managed when they cannot be avoided.

MSD has a policy and a procedure to help you and your manager identify and manage conflicts of interest that arise in the course of your work. You can find the policy and procedure for managing conflicts of interests on our intranet (doogle).

You must inform your manager if you have a relationship with someone you deal with in your role or someone we deal with at MSD that could cause or be seen to cause a conflict of interest.

Secondary employment and voluntary work – if you take on other work (paid or unpaid) or services while you work at MSD, you'll need to consider how it could affect your work here, and whether there is any potential or perceived conflict of interest. Talk to your manager about this. Refer to the Conflicts of Values, Interests and Politics policy for information on secondary employment and managing conflicts.

Respecting others

As an MSD staff member you need to make sure you respect the rights of other people, all the time. This includes any client, stakeholder, colleague or member of the public.

In particular, you must:

- treat each other with respect and courtesy
- show mana manaaki and look after the dignity of people
- support a positive and safe work environment free from any form of bullying, harassment or discrimination (refer to MSD's Positive Workplace policy and guides on our intranet (doogle)
- avoid acting in a way that could upset people, or cause harm or disruption
- not bring anything to work that could be seen as offensive to any person or group of people
- ensure any workplace relationships with colleagues don't have a negative effect on your work
- recognise MSD's commitment to the Treaty of Waitangi
- always be professional, fair and unbiased in the work you do, or the advice you give
- remember that everyone has the right to privacy and confidentiality
- make sure you don't abuse your position at MSD, or any power delegated to you in your role.

We understand that sometimes you may need to do something as part of your role that conflicts with your personal beliefs. If you find yourself in this position, talk to your manager. They will be able to discuss this with you and help you find the right solution.

Impartial

We must:

- maintain the political neutrality required to enable us to work with current and future governments
- carry out the functions of our organisation, unaffected by our personal beliefs
- support our organisation to provide robust and unbiased advice
- respect the authority of the government of the day.

Public Service Commission Standards of Integrity and Conduct: Impartial
https://www.publicservice.govt.nz/resources/code/?e200=1518-impartial

Political neutrality

While we work with the government of the day, we must also be able to work with future governments. This means we need to maintain the confidence of our current Minister and make sure the same relationship can be established with future Ministers. We do this by keeping politics out of our work and our work out of politics.

As public servants we have the same rights as other New Zealanders and may publicly express our own political or personal views. However, at the same time we need to work in a professional and politically neutral way.

Most people at MSD can be involved in social campaigns or the activities of political parties and other organisations without it affecting their ability to be impartial in the work they do.

Talk to your manager about your actual or intended political involvement. It's important to consider what you can do to avoid a perceived conflict with your work. This may include steps so that you are not identified as working for MSD or taking annual leave if you need time off for activities you are involved in.

For senior managers, people who have extensive contact with Ministers, and those responsible for interpreting and implementing government decisions we have to keep a balance and it is not appropriate to publicly express views about government policy related to their work area.

The Public Service Commissioner's guidance about political neutrality is available at **www.publicservice.govt.nz** or you can talk to your manager if you have any questions about what this means for you.

Commenting on government policy

MSD may view any staff members who publicly make strong or repeated criticisms of government policies as being unable to impartially implement, administer or advise on government policies.

For all staff, publicly expressing your personal view of government policy is unacceptable if you:

- disclose information gained by your work at MSD
- are or could be perceived to be representing MSD
- make personal attacks on a Minister, people at MSD or other Public Servants
- strongly or persistently criticise to the extent that it could be perceived that you cannot carry out your work in an impartial way.

Due to the nature of the roles, for Senior Managers, people working with Ministers, and those responsible for interpreting and implementing government decisions there is a greater responsibility to not publicly comment on government policy related to their work area.

Only people who are authorised by the Chief Executive or who have permission as part of their job can make public statements on behalf of MSD. This applies to responses to any media enquiry.

Private communications with Ministers or Members of Parliament

You have the same right to approach political representatives as any other person, but you must be clear that you are not representing MSD. Remember, any approach to a political representative about something that is not to do with MSD's work should be made with some sensitivity to your role as a public servant.

Any matters concerning MSD must go through the official channels.

Standing as a Member of Parliament

Public servants can seek election to Parliament but there are rules about this set out in the Electoral Act 1993. If you are thinking about putting your name forward for nomination as a constituency candidate or for inclusion on a party list, or if you have already done so, tell your General Manager, Regional Commissioner or the Group General Manager People (Human Resources). They will discuss this with the Chief Executive.

You can find more information on the Public Service Commission website **www.publicservice.govt.nz/resources/code** and in the Public Service Standards of Integrity and Conduct.

Responsible

We must:

- » act lawfully and objectively
- » use our organisation's resources carefully and only for intended purposes
- » treat information with care and use it only for proper purposes
- » work to improve the performance and efficiency of our organisation.

Public Service Commission Standards of Integrity and Conduct: Responsible
https://www.publicservice.govt.nz/resources/code/?e200=1520-responsible

Probity

When we deal with public money and resources, there is a standard of behaviour expected of us. This is called probity.

Probity means we have shown integrity and professionalism in using public money to do our work.

Probity isn't about setting a list of rules; it's about showing we have used good judgement and a sensible process to make our decisions around how we spend money.

When spending public money, you can show probity if your expenditure:

- is reasonable
- demonstrates value for money
- is relevant to what we do, or to our goals
- can satisfy the questions of anyone who asks about it, including the public.

If you have questions about probity or how to apply it in your role, talk to your manager.

MSD's financial policies are available on our intranet (doogle).

Information and confidentiality

We need to keep all MSD information secure, including personal information about our clients, their families or other organisations.

How we treat this information – collect it, store it, share it and use it – affects how the public trusts us and whether they are willing to continue to share their information with us so we can do our jobs properly.

MSD has a number of policies and procedures in place to protect information and to help us manage information appropriately.

This includes complying with the:

- Official Information Act 1982
- Privacy Act 2020
- Public Records Act 2005.

If information is inadvertently or unintentionally released or disclosed, take action straight away to minimise any risks, or impact on people. You must also contact MSD's Privacy Team to report the incident. They can give you further advice about handling it.

Refer to MSD's privacy and security policies on our intranet (doogle).

You can find more about MSD's information policies on our intranet (doogle), including our IT security policies (End User Security Policy).

Accessing information

Each of us must take care to ensure MSD and client information is only accessible to authorised people for authorised use.

Make sure you always observe people's right to privacy when you are dealing with their personal information.

- You must only access client information or records for legitimate work purposes.
- You must not access your own record or the record of a friend, relative, colleague or acquaintance for any reason, even if the person asks you to, including if you're just interested or browsing.
- Accessing information also includes processing actions on records. You must not undertake any processing action within your own record or the record of any current or former client, including your own record if you're a current or former client of MSD, without a legitimate business reason.

This applies to any information we hold in any form. If you are not sure whether it is appropriate for you to access information, always check with your manager first.

Misuse of information

Misuse of information includes accessing, falsifying, requesting, or sharing of information without a business purpose. To get the most valid information and to protect people's privacy, information should generally be requested from the person themselves, rather than a third party.

If you are found to have misused or falsified MSD information, formal disciplinary action will be taken, which may include dismissal.

MSD has a zero tolerance policy for the misuse of personal information. Any staff member found to have sold or deliberately given client information to any unauthorised person will be dismissed and the matter may be referred to police.

You can find more information about this on our intranet (doogle).

Trustworthy

We must:

- be honest
- work to the best of our abilities
- ensure our actions are not affected by our personal interests or relationships
- never misuse our position for personal gain
- decline gifts or benefits that place us under any obligation or perceived influence
- avoid any activities, work or non-work, that may harm the reputation of our organisation or of the State Services.

Public Service Commission Standards of Integrity and Conduct: Trustworthy
https://ssc.govt.nz/resources/code/?e200=1522-trustworthy

Client relationships

When we work for a government department it is important to be aware of how our relationships can affect the way we do our jobs or the reputation of MSD.

You must inform your manager if you have a relationship with someone you deal with in your role or someone we deal with at MSD that could cause, or be seen to cause, a conflict of interest.

Disclosing and managing these relationships is important to ensure the public's trust in MSD is well-founded and conflicts of interest are appropriately managed.

MSD has a vital role in our communities to help New Zealanders to be safe, strong and independent. Because of this, if you have sexual contact with, or abuse in any way, a child or young person we have a professional relationship with, you will be dismissed and the matter may be referred to police.

Fraud

As an MSD staff member, you must not commit, condone, encourage or be directly associated with any type of fraud.

MSD has a zero tolerance policy for staff fraud and misuse of client information (available on doogle). In every case where a staff member is found to have defrauded MSD, they will be dismissed and the matter may be referred to police. In addition to any penalty the Court might impose, all money fraudulently obtained will have to be repaid in full.

If you know, or think you know, that someone is involved in fraud against MSD, tell your manager, the Internal Fraud Unit or Fraud Intervention Services.

Prior or pending convictions

If you have a conviction we didn't know about before we hired you, or you weren't truthful about having a conviction, we may take disciplinary action which could result in dismissal.

This does not apply to anything covered by section 7 of the Criminal Records (Clean Slate) Act 2004.

You must tell your manager if you have any convictions or charges laid against you while you work for MSD.

Roles requiring National Security Clearance

People in roles which require National Security Clearance must obtain and maintain this clearance at the appropriate level.

Gifts and rewards

Receiving a gift or reward for doing your role could be seen as a bribe or as a way of making you obligated to another person or organisation. As a general rule you should not ask for or accept a gift or reward.

Consider the intention of the gift and whether it is related to a cultural practice. Some occasions (such as a hui) may require an exchange of gifts. We are committed to meeting the needs of different cultures and if a gift is offered in these situations, it should be accepted on behalf of MSD.

Refer to MSD's Gifts, Donations and Koha Policy when giving or receiving a gift.

Staff who are also clients

If you receive payments or services from MSD, you must make sure anything you do as a client is honest and lawful.

It is your responsibility to give the Staff Assistance Unit full details about your circumstances or any changes in your circumstances to ensure you receive the correct entitlement.

Exemptions and other considerations

For a small number of staff, obligations under the Code of Conduct must be considered alongside other requirements eg for staff to act independently from MSD or to uphold the maintenance of the law. MSD may consider exemptions on a case by case basis to specified sections of the Code of Conduct, taking ethical and legal considerations into account.

Any exemptions will be approved by the relevant Deputy Chief Executive and the Group General Manager People (Human Resources).

Breaches of the Code of Conduct

We need to identify breaches or potential breaches of the Code as soon as possible. We will always make sure any disciplinary process is impartial, fair, prompt and consistent. We will consider each case on its merits, including reviewing the reasons for the breach and taking into account the individual circumstances of each case before deciding on the action to take.

Reporting breaches of the Code of Conduct

If you find out about a breach or possible breach of either the Public Service Standards of Integrity and Conduct or this Code of Conduct, you should:

- think carefully about how you can deal with the situation responsibly
- discuss the issue or situation with your manager as quickly as possible – they may have additional information you might not know, so trust them to know the best way to deal with things.

Talk to your manager to report a breach of any other MSD policy, procedure, standard or guideline, unless another process is provided.

If you don’t think you can talk to your manager, or if the situation remains unresolved, then you can talk to another MSD manager or the Group General Manager People (Human Resources).

If you need access to confidential counselling, MSD’s Employee Assistance Programme (EAP) is voluntary, private, free, confidential and available to all MSD staff. You can find more details on EAP on MSD’s intranet (doogle).

Managers who are advised of a breach or a possible breach will deal with the alleged breach in accordance with MSD’s policy. This means anyone alleging a breach or who is being investigated for a breach of the Code of Conduct will be given adequate notice of meetings, have an opportunity to be heard, and have the right to representation and/or have a support person present at meetings.

Privacy breaches

Refer to the Information and confidentiality’ section of the Code of Conduct and MSD’s intranet (doogle) for reporting a privacy breach or near miss.

Reporting serious wrongdoing

In some cases, a breach of the Code of Conduct may also be serious wrongdoing under the Protected Disclosures Act 2000. If this is the case, you can use the MSD's Protected Disclosures procedures to report the incident or action and receive the protections of the Act. There is information about protected disclosures on our intranet (doogle).

If you think MSD has not met its obligations under the Code

If you think MSD has not met its obligations, follow the same process as the one to report breaches of the Code of Conduct (as set out above).

Once you have told us about your concerns, we will:

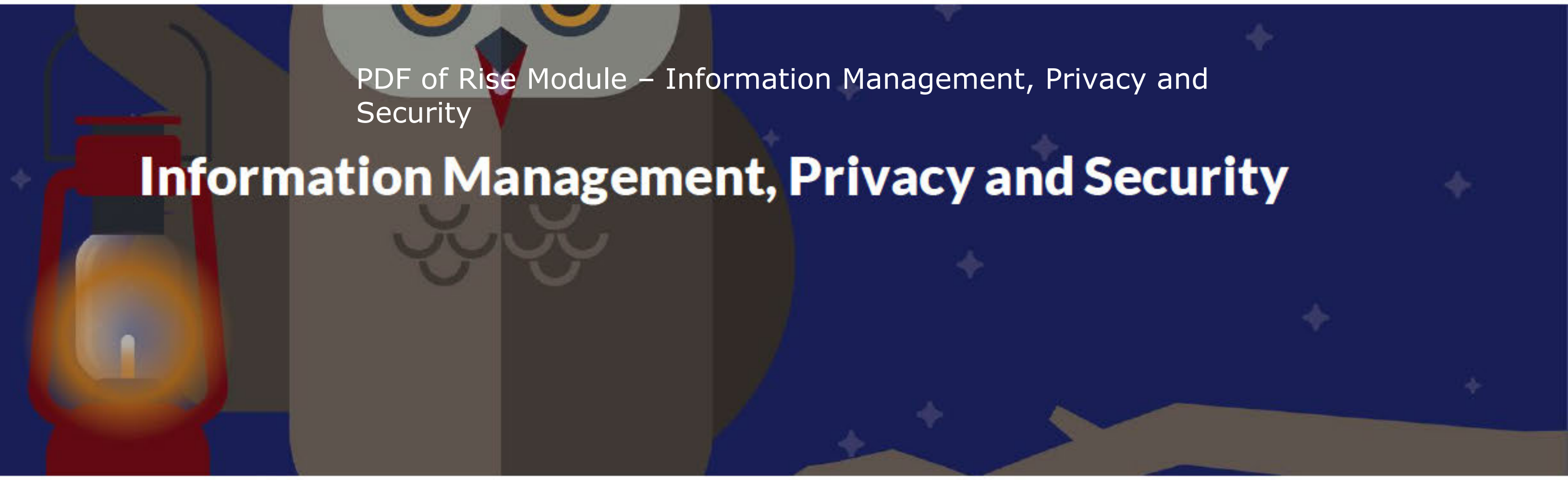
- treat your concerns confidentially, investigate them promptly and appropriately, and take action as necessary
- where appropriate, let anyone affected by an allegation know about it and ask for their explanation
- consider the use of a neutral third party to resolve the issue, if appropriate
- let you know if an investigation or action has started and stay in regular contact, if appropriate
- let you know about the outcome, where appropriate.

MSD will make every effort to maintain the confidentiality of an individual making a protected disclosure. This is set out in our Protected Disclosures policy.

Remember, you can also face disciplinary action for breaching other MSD policies, procedures and guidelines.

If you are unsure about how to deal with an ethical issue, discuss it with your manager. If your manager is involved, discuss the issue with your manager's manager or any senior manager.

MINISTRY OF SOCIAL
DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA



PDF of Rise Module – Information Management, Privacy and Security

Information Management, Privacy and Security

Nau mai, haere mai and welcome

Welcome to the Information Management, Privacy, and Security online training module.

In this module, you will cover:

- what information management is and why it is important
- protecting information
- information privacy and sharing
- how to recognise and report a privacy, information, or IT security breach
- two scenarios
- next steps and where you can find more information.

This module will take you 15-20 minutes. There is audio so please use a set of headphones to not disturb your colleagues.

Click on 'Start Course' (above) or 'Introduction' (below) to begin.

Introduction

Managing our information

Rights to access information

- Recognising and reporting information breaches
- Scenario one - Information management
- Scenario two - Privacy and security
- Conclusion and handy links
- Test quiz

Lesson 1 of 8

Introduction

What information management is and why it is important

To get an overview on why information management is important at MSD, please watch the 30 second video below.

Note: The volume of this video is a bit loud. We recommend turning down the volume on your headset before watching it.

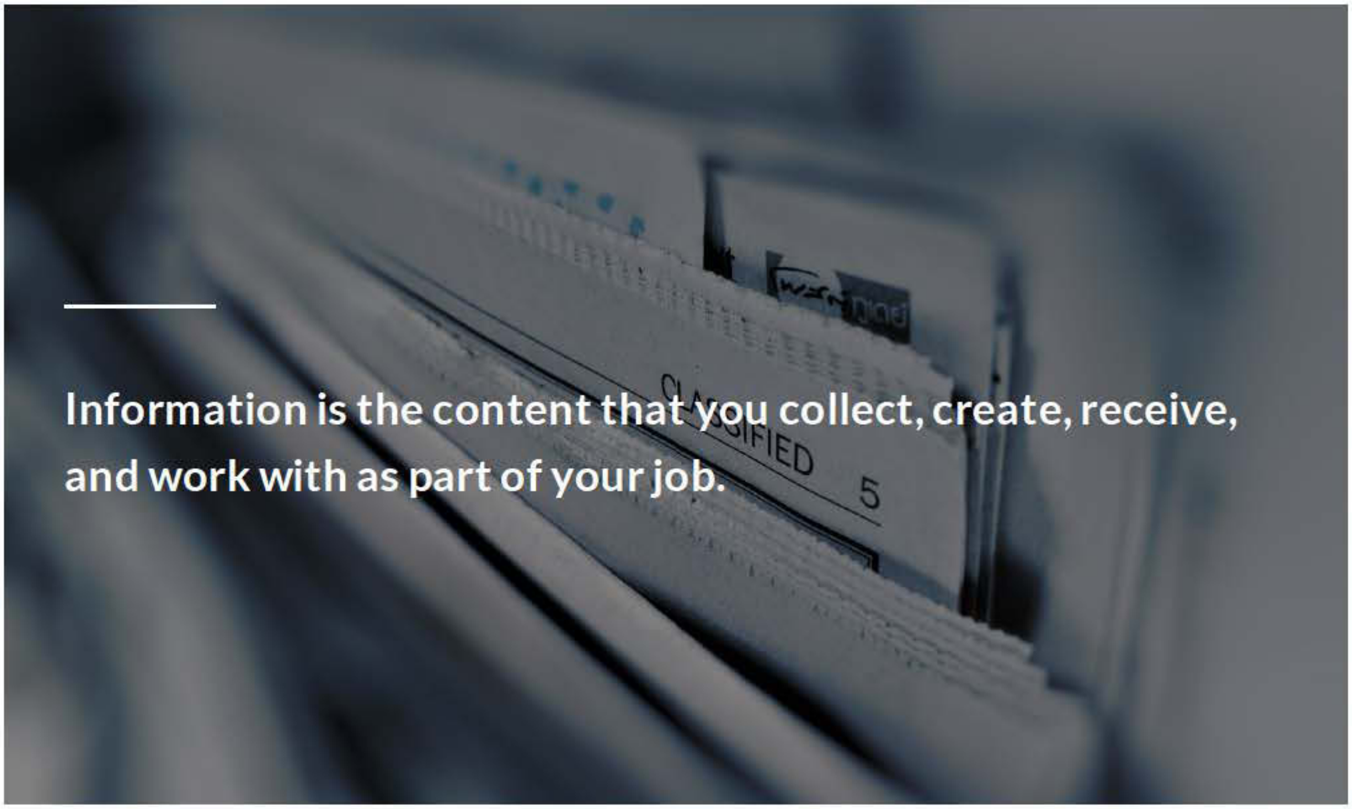
Download the transcript

Our duty under the Privacy Act 2020 and the Public Records Act 2005 is to safeguard New Zealanders' information. As Ministry staff we all have a part to play in meeting our obligations.

The public expect the Ministry to look after their information. If we don't meet these expectations, we lose the trust and confidence of New Zealanders to deliver our services.

Lesson 2 of 8

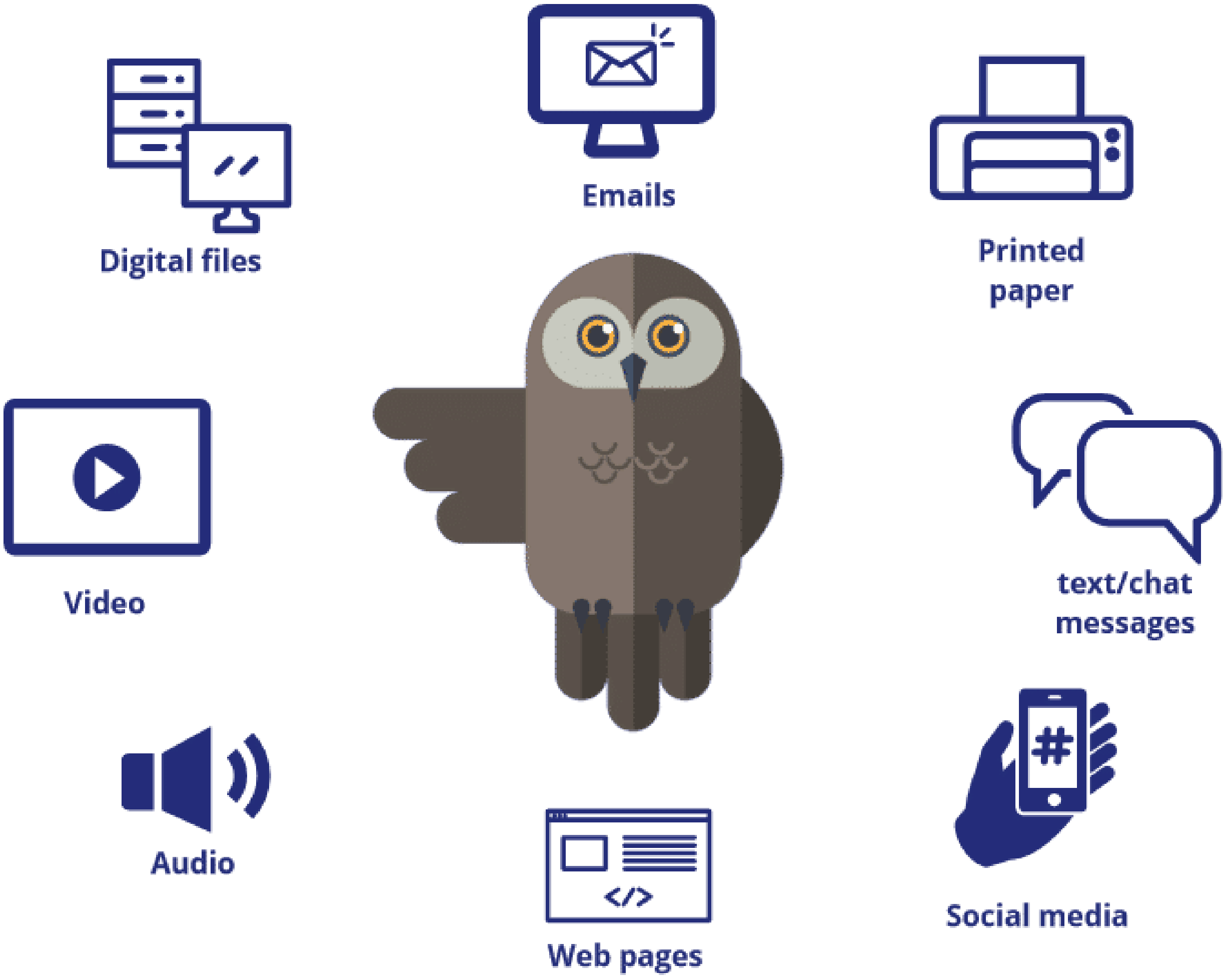
Managing our information



Information is the content that you collect, create, receive, and work with as part of your job.

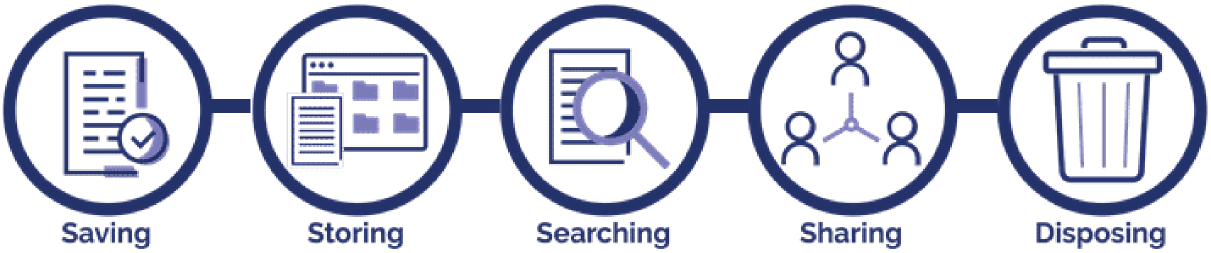
Information comes in all forms and shapes.

We hold many types of information including information from and about our clients, as well as corporate information that we create and use to manage the business of MSD.



Information management

Information management is about how we create, collect, organise, use, secure, control, share, maintain, and appropriately dispose of this information.



Lets have a look at the information lifecycle and the phases of it.

Saving

You must save information you receive or create which relates to your work on behalf of MSD that provides evidence of our business activities or decisions.

Emails we send and receive that record significant actions or decisions must be stored in the appropriate repository, such as Objective.

For more information on saving, look at this page on **Doogle**.

Storing

You must only store information in approved MSD information systems, such as Objective or line-of-business systems (e.g. CMS). Avoid keeping it in locations that cannot be accessed by others, such as desktops, hard drives, email inbox or folders, or personal drives.

Digital information is considered the authoritative source and we should avoid keeping paper copies of digital records.

For more information on storing, look at this page on **Doogle**.

Searching

Information is created and received every day. Making it discoverable and using searches to find relevant information is important. It enables MSD to reuse information and gain insights to deliver better products and services for New Zealanders.

At MSD, a large number of documents are created and saved into Objective every day. This is one reason why naming information well is important. Giving your documents meaningful names will make them easier for you and your colleagues to find when you're running searches.

For more information on naming conventions/naming information, look at this page on **Doogle**.

Sharing

At MSD, access to information must be open by design to all staff, and restricted by exception. This means that information is accessible to all MSD staff and is restricted only where there are legitimate reasons to do so (e.g. personal information). This enables knowledge sharing and reuse of information.

When sharing information with your colleagues, whenever possible, share a link to the original content, rather than sending a copy.

When sharing externally, we need to ensure we are protecting our information, including our clients' rights and privacy, by using an approved sharing mechanism that allows us to share information securely.

For more information about sharing, look at this page on **Doogle**.

Disposing

While we are all responsible for creating and maintaining full and accurate information, it is equally important that we dispose of information when we are legally able to do so. Different types of records have varying lengths of time they need to be kept before they can be disposed of. This ranges from 'as long as MSD needs it' to 'transfer to Archives for permanent retention'.

Information can only legally be disposed of by the IM team.

The types of information described below have short-term or no value and can be deleted by staff when no longer required:

- Short term value - Information that is only needed for a short-term period to support business transactions, decisions or activities, and does not record or add valuable context to them in the long term

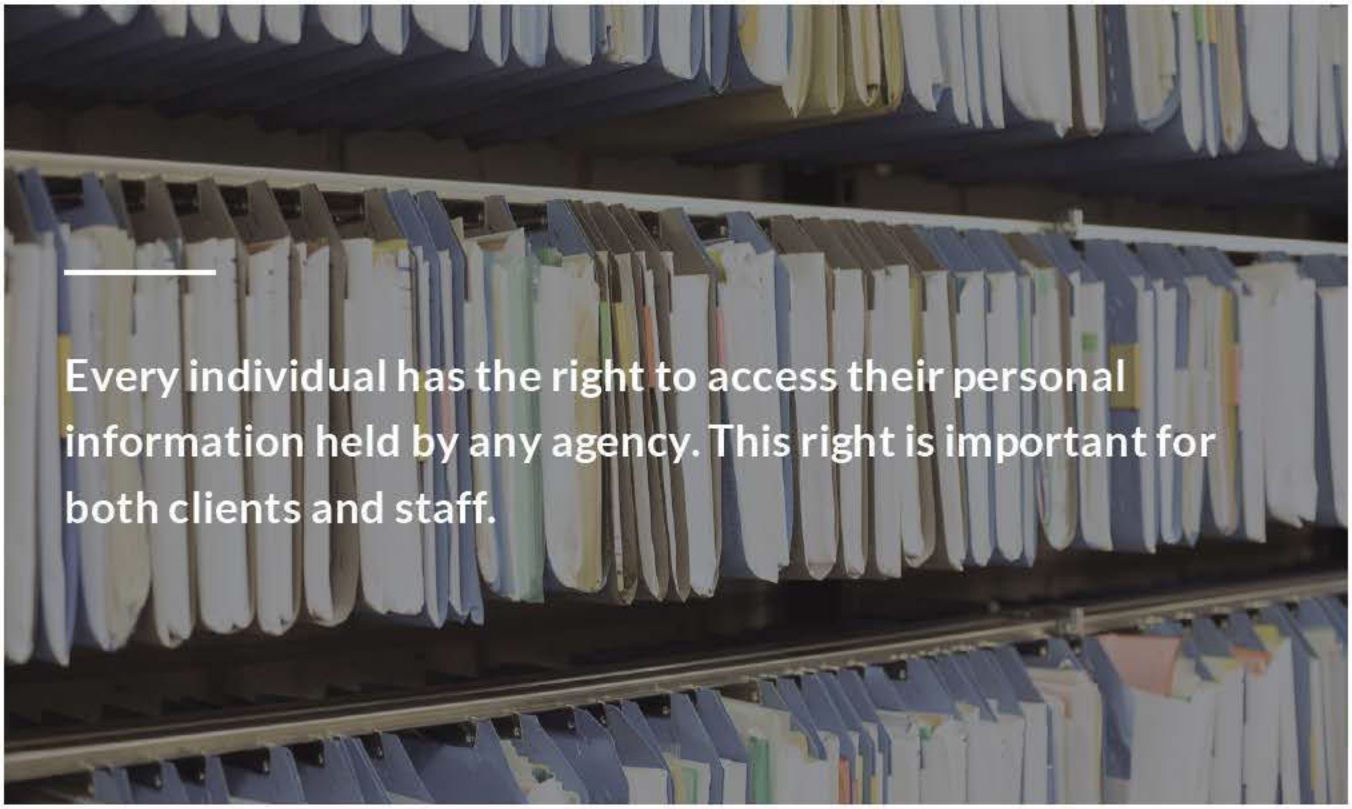
- Duplicates - Information that is a duplicate, and a copy has been saved elsewhere in our systems
- No business value - Not business information as it does not provide valuable context to business transactions, decisions or activities.

For more information on disposing, look at this page on Doogle.

You can find more information about managing Ministry information on Doogle, but if you have any questions, contact the IM team.

Lesson 3 of 8

Rights to access information



Every individual has the right to access their personal information held by any agency. This right is important for both clients and staff.

Providing access is important because it holds us to account about what we do in our roles, how we handle and treat information, and the decisions we make about people. Providing a client access to the information we hold enhances trust and enables people to query the information we have that might be wrong.

Conversations, emails, notes, opinions, and decisions you make about a person can be requested at any time. Remember to always be respectful, and keep records professional, relevant, accurate and up to date.

Making a request

A person can make a request for their information in a variety of ways, for example:

- via an email or text direct to a case manager
- via a social media or website channel owned by MSD
- in a written letter
- verbally, over the phone or in person.

Providing access

If we have the information and it's easy to provide immediately, then we should provide it immediately. Usually requests must be acknowledged, and access provided within 20 working days from the day it was received by the agency or the Ministry. An extension may be granted if the information is difficult to access.

There is no option not to provide access unless specific exceptions or withholding grounds apply. Not providing access to information, could be a breach of the Privacy Act.

Where to find more information

There are clear guides on Doogle on how to handle a request for personal information. Follow the process already established, and if in doubt about what can be released, talk to your manager or a member of the Privacy and Information Sharing team.

Lesson 4 of 8

Recognising and reporting information breaches

Privacy and Security breaches can happen for a variety of reasons.

The Ministry has technology to both protect against hackers and prevent accidental information loss. However, hackers or scammers sometimes use sophisticated methods to target individuals in order to obtain information. This along with our often-hectic working lives can lead to things going wrong and a security or privacy breach can happen. We are only human and as humans we all make mistakes. What is important though is how we handle the situation when things do go wrong.

It is really important to contain the impact of an information breach. The number one thing you can do if you think a breach has occurred is to report it to your manager immediately. You will not get in trouble for this.

The Ministry has teams and processes for dealing with breaches and, once notified, these teams will help and support you to manage the breach for the Ministry. Don't worry if you're not sure if you are dealing with a security or privacy breach, the most important thing is to contact your manager who will in turn contact one of the specialist teams and they will work together to contain and resolve any breach.

Examples of a security or privacy breach

- An email sent to an incorrect recipient due to an email address mistype, or out-of-date address held on record, resulting in a loss of control and the disclosure of personal information.
- Losing a physical file containing client or Ministry information in a public place.
- Sending personal information as a result of a phishing attack to an unknown person.
- Scam (phishing) and SPAM emails, phone calls and texts resulting in personal information being disclosed.

Who to contact

If you think an IT Security breach has occurred, tell your manager who then should contact the **Service Desk** or the **IT Security team** directly for advice or to report the issue.

If you think a Privacy breach has occurred, tell your manager who then should contact the **Privacy Officer** to report the issue.

For more information, look at this **Doogle** page.

Don't worry if you're not sure if you are dealing with a security or privacy breach, the most important thing is to tell your manager.

Lesson 5 of 8

Scenario one - Information management

Now we're going to go through a scenario for information management.

Answer the questions below.

Background

You have been asked to do a stocktake of supplies in the basement at your work and came across some unsecured boxes of MSD files.

1. What is the first thing you should you do?

○ Tell the landlord.

○ Close the door and not worry about it.

○ Talk to your manager about what you should do.

SUBMIT

🔒 Complete the content above before moving on.

Your manager gave you approval to review and register all the files in the basement including client files. They also mentioned that if you have any questions, you can reach out to the Information Management team.

2. As you go through them, you find a file that has the same name as your auntie. What do you do?

○ Have a quick peek inside.

○ Tell your manager so they know there could be a potential conflict of interest.

○ Take photos of the information inside and send them to your auntie.

SUBMIT

Complete the content above before moving on.

Your manager believes there is no issue as long as you aren't looking inside the files.

After you report back to your manager about the contents, they realise that the files in the boxes need to be registered. This is important so we know what information we hold and where to source them in the future. You register the boxes and send them offsite to the approved storage facility.

3. Some loose papers and files have been identified as ready for destruction. What do you do?

○ Dispose of it in the blue destruction bin.

○ Throw it in the big communal waste bin around the corner.

○ Re-use the other side of the paper for taking notes.

○ Create garlands out of them for the office Christmas decorations.

SUBMIT

🔒 Complete the content above before moving on.

4. How would you avoid situations like this in the future? Tick all that apply.

□ Register and store files in an approved offsite storage facility or locked cabinet onsite.

□ Check that it’s not already saved somewhere. If it’s not, scan it and save it into approved system, then throw away the original paper.

□ Dispose of paper files without an assessment, since the future is digital.

□ Lock the basement and not create a register of the files.

SUBMIT

🔒 Complete the content above before moving on.

Thanks to you, the files are now in a secure and dedicated storage facility, and is only able to be accessed by the appropriate authorised personnel via a tracked process.

Lesson 6 of 8

Scenario two - Privacy and security

Now we're going to go through a scenario for privacy and security.

Answer the questions below.

Background

A client has been disputing entitlement to a supplementary payment. She has spoken to our call centre several times over the last six weeks . She is frustrated and worried about her and her child's safety. We know that she is living in temporary housing having just separated from her violent partner and is in the process of securing a rental property.

During a recent call, she asked for all call recordings she has had with us. We told her we can only provide call recordings from the last 90 days, because they're deleted after 90 days. She does not tell us why she wants them.

Can a client make a verbal Privacy Act request for call recordings? (tick all that apply)

□ Yes, a voice recording is considered personal information.

□ Yes, we hold this information so it must be considered for release.

□ Yes, the request was made verbally and clarified during the call.

□ No, she has not told us why she wants the recordings.

□ No, we have been very rude and dismissive in one of the calls so best not provide her with this recording.

SUBMIT

Complete the content above before moving on.

The staff member makes a file note on her CMS record that a request has been made. They know there's a time restriction to provide a response and quickly escalates the request to their manager. The manager follows the process required to pull the call recordings and have copies made.

How many days do we have to respond with our decision?

○ 30 days.

○ 20 working days.

○ 10 working days.

SUBMIT

🔒 Complete the content above before moving on.

The calls are downloaded and ready to be checked prior to release. The manager asks their staff member to confirm with the client what format they would like the recordings in and what address to send the parcel to.

The staff member was unsure what address to send the parcel to. They should:

○ Send it to the last address in CMS.

○ Call the client and confirm their preferred address for delivery.

○ Call the client's partner and check what address they suggest we send it to.

SUBMIT

🔒 Complete the content above before moving on.

The client wants the recordings on a USB. Prior to copying the recordings to the USB, the manager listens to the calls and discovers the call where one of the staff was dismissive and rude to the client. They want to omit this recording entirely as it's not a good look for the team.

The manager is worried this reflects badly on the team or could be disclosed to the media. Can they delete it from the recording?

○ Yes, delete it. It's not a good look for the team.

○ No – this is the client's information and should be provided despite it being unprofessional.

SUBMIT

🔒 Complete the content above before moving on.

The remaining files are loaded to the USB drive which is password protected. The password is written onto a PostIt note and put into the envelope with the USB. The envelope is bundled into the courier bag and left at reception ready for the 3pm courier pickup. Track and trace was applied.

Something is wrong – what is it?

○ Password protecting the USB.

○ Writing the password on a Post-It note.

○ Enclosing the password in the same envelope with the USB.

○ Using track and trace.

SUBMIT

Complete the content above before moving on.

A few days later the client emails back to let us know that the parcel has not been received. The staff member checks the CMS record and the reception dispatch processes and confirms track and trace was applied. They contact the courier company who confirm the parcel was lost at their distribution depot warehouse.

There appears to be some kind of breach – what could the staff member do? (Tick all that apply)

□ Report it to their manager.

□ Complete the Notify a privacy or IT security incident form on Doogle.

□ Call someone in the Privacy team or email the Privacy Officer.

□ Follow the step by step support on Doogle.

SUBMIT

Lesson 7 of 8

Conclusion and handy links

Congratulations

Well done. You have completed this module on information management, privacy and security.

You have covered:

- what information management is and why it is important
- protecting information
- information privacy and sharing
- how to recognise and report a privacy, information, or IT security breach
- two scenarios.

Main points

The Ministry holds information about people and uses information that impacts their lives. The information we hold and use is **taonga** (a treasure), and as its guardians we must both use it responsibly and protect it while it is in our care.

All MSD staff are responsible for managing information and keeping it safe through its lifecycle.

If you think an information breach has occurred, you must report it to your manager immediately. You will not get in trouble for this.

Every individual has the right to access their personal information held by any agency. This right is important for both clients and staff.

Handy links

The **Information Hub** is a collection of Doogle pages by the Information Group. It has guidance, tools and resources to enable MSD staff to work with information while protecting ourselves, our clients, and our information assets from risk.

Contact Information Management team (**infohelp@msd.govt.nz**) for advice creating, collecting, organising, controlling, storing, maintaining and disposing of information.

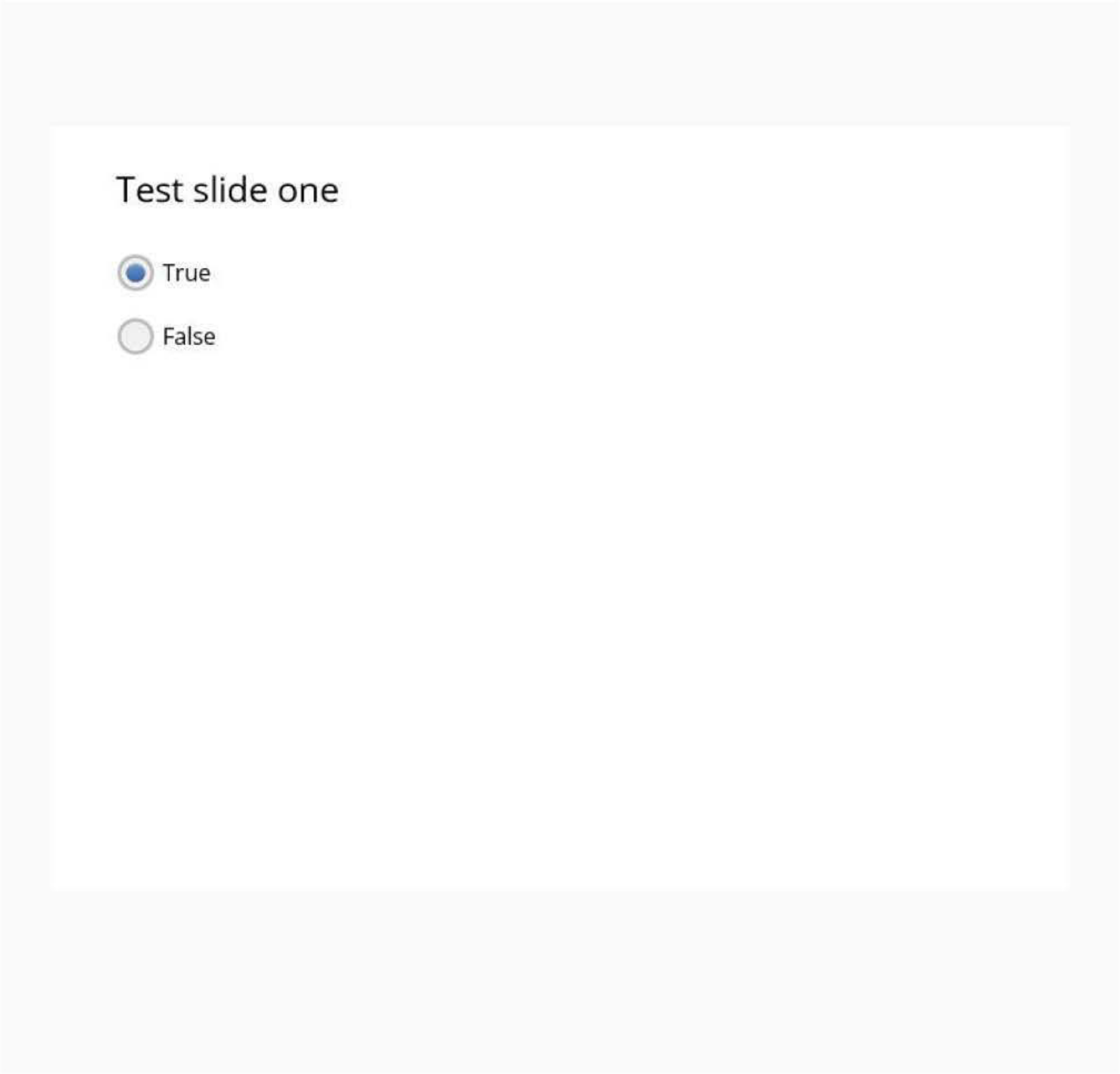
Contact the Privacy Team (**PrivacyOfficer@msd.govt.nz**) for advice if you think a privacy breach has occurred.

Contact the IT Security Team (**IT_Security@msd.govt.nz**) for advice if you think a security breach has occurred.

You can now close the module.

Lesson 8 of 8

Test quiz

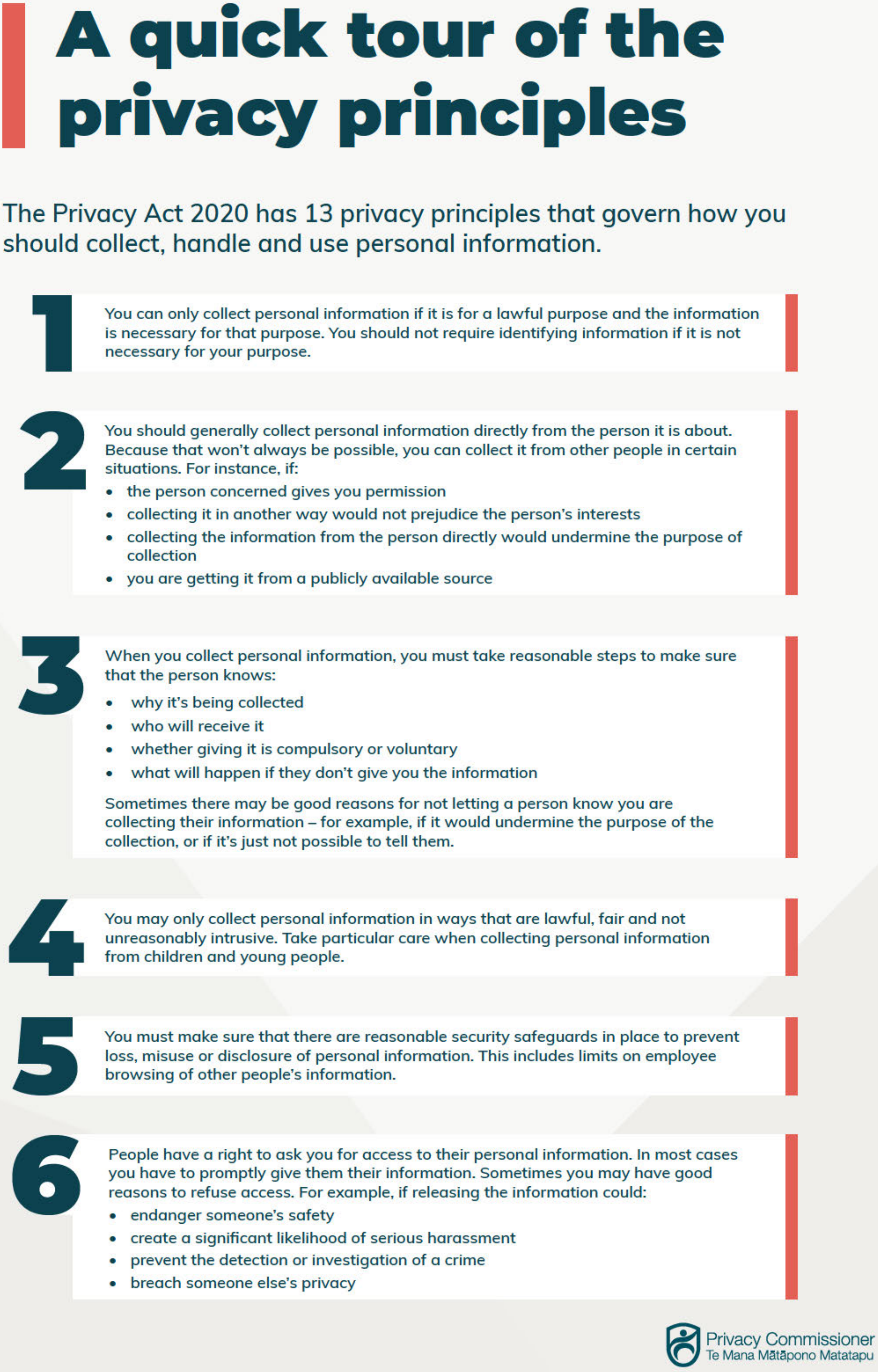


Test slide one

● True

○ False

Office of the Privacy Commissioner – a Quick tour of the privacy principles



A quick tour of the privacy principles

The Privacy Act 2020 has 13 privacy principles that govern how you should collect, handle and use personal information.

1 You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

2 You should generally collect personal information directly from the person it is about. Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:

- the person concerned gives you permission
- collecting it in another way would not prejudice the person's interests
- collecting the information from the person directly would undermine the purpose of collection
- you are getting it from a publicly available source

3 When you collect personal information, you must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if they don't give you the information

Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

4 You may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

5 You must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

6 People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:

- endanger someone's safety
- create a significant likelihood of serious harassment
- prevent the detection or investigation of a crime
- breach someone else's privacy

Privacy Commissioner
Te Mana Mātāpono Matatapu

7

A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if you don't agree that it needs correcting, you must take reasonable steps to attach a statement of correction to the information to show the person's view.

8

Before using or disclosing personal information, you must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

9

You must not keep personal information for longer than is necessary.

10

You can generally only use personal information for the purpose you collected it. You may use it in ways that are directly related to the original purpose, or you may use it another way if the person gives you permission, or in other limited circumstances.

11

You may only disclose personal information in limited circumstances. For example, if:

- disclosure is one of the purposes for which you got the information
- the person concerned authorised the disclosure
- the information will be used in an anonymous way
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to avoid a prejudice to the maintenance of the law

12

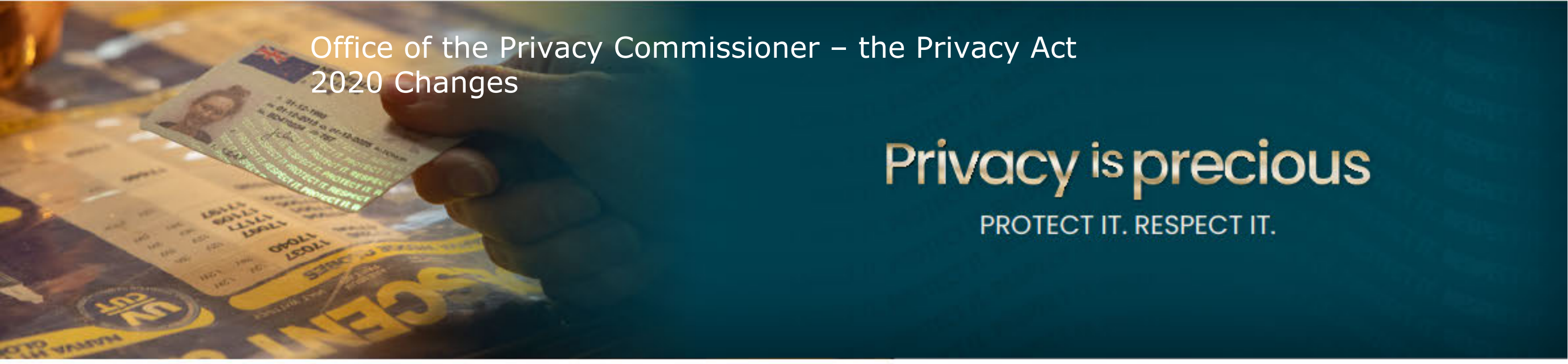
You can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
- the information is going to a place with comparable privacy safeguards to New Zealand
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there aren't adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

13

A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. You can only assign your own unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation. If you assign a unique identifier to people, you must make sure that the risk of misuse (such as identity theft) is minimised.



THE PRIVACY ACT 2020 CHANGES

New Zealand's Privacy Act has been modernised to reflect changes in the wider economy and society and to ensure it is fit for the technological world in which we live. This is a very brief summary of the key changes in the new Act.

Notifiable privacy breaches

If a business or organisation has a privacy breach that has caused serious harm to someone (or is likely to do so), it will need to notify the Office of the Privacy Commissioner as soon as possible. It is an offence to fail to notify the Privacy Commissioner of a notifiable privacy breach.

If a notifiable privacy breach occurs, the business or organisation should also notify affected people. This should happen as soon as possible after becoming aware of the breach.

Compliance notices

The Privacy Commissioner will be able to require a business or organisation to do something, or stop doing something, if it is not meeting its obligations under the Privacy Act.

Binding decisions on access requests

The Privacy Commissioner will now be able to make decisions on complaints relating to access to information. This will mean a faster resolution to information access complaints.

Disclosing information overseas

A New Zealand business or organisation may only send personal information to another country if that country has similar levels of privacy protection to New Zealand, or the person concerned is fully informed and gives their permission.

Extraterritorial effect

The Privacy Act has extraterritorial effect. This means that an overseas business or organisation may be treated as carrying on business in New Zealand for the purposes of its privacy obligations – even if it does not have a physical presence in New Zealand.

New criminal offences

It will now be a criminal offence to:

1. mislead a business or organisation by impersonating someone, or pretending to act with that person's authority, to gain access to their personal information or to have it altered or destroyed.
2. destroy a document containing personal information, knowing that a request has been made for that information.

The penalty in all cases is a fine up to $10,000.

Further resources

You can find further resources on our website: privacy.org.nz/2020

Privacy Commissioner
Te Mana Mātāpono Matatapu