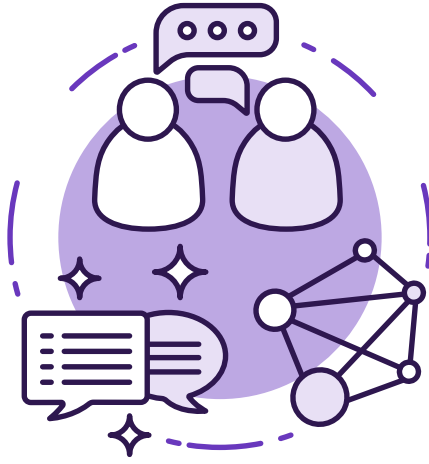Te Kāwanatanga o Aotearoa
New Zealand Government

GCPO Guidiance

Sharing information at multi-agency meetings

Sharing information appropriately at multi-agency meetings builds public trust and confidence, enables effective and efficient delivery of interventions and support services, and leads to better outcomes for individuals.

Contents

Purpose of Guidance

The purpose of this guidance is to help you understand:

- what a multi-agency meeting is
- how to set up information sharing at multi-agency meetings
- what to think about before you share information at a multi-agency meeting

The guidance will help you share information at a multi-agency meeting in a considered and people-focused way.

We have also created an information sharing protocol template to help to support agencies with documenting their sharing activity. The guidance aligns to the structure of that template so you can develop your information sharing protocol in a systematic and consistent manner.

Guidance Audience

The guidance can be used by:

- Public sector agencies, including:
  - frontline staff
  - regional staff
  - national Office staff
- Organisations working with government agencies

What is a multi-agency meeting?

A multi-agency meeting is a meeting where different agencies and organisations come together for a common purpose. These meetings can be one-off events or occur regularly.

To provide services and deliver effective outcomes, agencies and organisations often need to share information (both verbally and in written form) about individuals. Sharing information enables them to understand and quantify the extent of a problem and then identify appropriate and effective supports, interventions, and services.

Examples of multi-agency meetings include:

Police led multi-agency meeting to reengage youth offenders in education or employment

There has been a significant increase in residential burglaries committed by youth in a small geographical area. Local police would like to identify, if possible, the cause of the increase in offending, and work with the youth offenders to reengage them with education or employment opportunities.

To achieve this, police will need to work closely with local non-government support organisations, and government agencies who also have an interest in seeing children and young people thriving and achieving — for example the Ministry of Education, Ministry of Social Development and Oranga Tamariki.

Regular multi-agencies meetings will enable police to share relevant information with appropriate agencies and organisations. This will help identify and implement effective supports and interventions.

Education led multi-agency meeting to identify learning support services

School attendance has been dropping over the last few years. The Ministry of Education (the Ministry) wants to understand the drivers behind the reduction in attendance rates. They want to implement effective student focused interventions to encourage students to attend school regularly.

To achieve this, the Ministry will need to work closely with schools, learning support service delivery partners, other government agencies — for example Oranga Tamariki, police, and non-government support organisations. The drop in attendance rates is a national problem requiring a nationwide approach.

Regular multi-agency meetings will enable the Ministry to share relevant information with appropriate agencies and organisations. This will help identify and implement effective supports and interventions. To ensure a consistent national approach to the sharing of information for these purposes, the Ministry will set up an information sharing protocol that is followed at all meetings throughout the country.

Sharing information at multi-agency meetings

Sharing information about individuals at multi-agency meetings can be challenging when there are no clear policies and procedures to follow. Everyone knows the consequences of sharing too much can be significant. But so can the consequences of sharing too little.

Privacy is not about keeping things secret. It's about getting the right information to the right people in a timely manner.

The way to be confident you're doing the right thing is to embed best practice information sharing into the governance and operation of multi-agency meetings. That will protect the people you're sharing information about and help you meet the objectives of your multi-agency meeting effectively and efficiently. It simply becomes the way you work.

We strongly recommend that all multi-agency meetings, especially those designed to operate over a period of time, have an information sharing protocol in place.

Why we need multi-agency meeting information sharing protocols

Information sharing is a critically important activity for government agencies.

Good information sharing practices, including the development and use of multi-agency meeting information sharing protocols:

- build awareness within an agency of what information is being shared, who the information is being shared with and for what purpose
- create transparency and build public trust and confidence in how agencies are sharing personal information
- enable agencies to deliver effective, fit-for-purpose public services that improve outcomes for individuals.

Protocol purposes and what they record

The purpose of a multi-agency meeting information sharing protocol is to document authorised sharing of information and ensure all attending agency representatives are aware of what information can and is being shared, for what purposes and under what legal authorities.

A multi-agency meeting information sharing protocol records:

- the purpose of the meeting
- the information being shared
- the legal authority the sharing is permitted under
- who the information will be shared with and for what purpose
- the controls and mechanisms that ensure personal information is shared safely and used appropriately.

Benefits of an information sharing protocol

The information sharing protocol helps attending agency representatives confidently share personal information in a timely manner. It also helps them to pause and make a confident judgement call when proposed information sharing within the meeting setting may create privacy risks.

Using our best-practice information sharing protocol template will enable you to show that the attending agencies have taken a privacy by design approach to information sharing practices. It's important to be able to show you have carefully considered the purpose, use and on-going management and protection of individuals' information.

From a practical perspective, recording how the information sharing works in the protocol also makes sure that the attending agencies and their representatives have the same understanding about what's happening and why.

Using the information sharing protocol demonstrates that attending agencies have taken a privacy by design approach to sharing information.

About the information sharing protocol

Individual multi-agency meetings can adapt it for their own needs if they have to, but the template captures the key things you have to think about. The majority of the protocol will remain the same for each multi-agency meeting setting.

How the template works

Most of the time associated with developing a multi-agency meeting information sharing protocol is spent working through the purpose, information requirements, legal authority, use and appropriate controls.

Use the next section of this guidance to help you know what to write.

Once this thinking has been completed and agreed between agencies, just complete the areas of the template marked with an asterisk (*).

The protocol template contains drop-down lists to reduce the time spent manually entering information. There's also the functionality to manually enter information such as names of attending agencies.

We've included instructions at the start of the template document to help you use and understand this functionality.

Develop your multi-agency meeting information sharing protocol

When setting up a multi-agency meeting it is vital that you think about and set up your information sharing practices correctly. The time and effort spent on setting things up at the beginning will make it easier to share what you need to share, without harming the people you are intending to help.

Use this guidance to complete the multi-agency meeting information sharing protocol template. The guidance walks through each section of the template and asks questions that agencies need to consider.

Multi-agency Meeting - Information Sharing Protocol Template

Meeting Purpose

A clear purpose is key. Your meeting purpose is the foundation on which the rest of your information sharing activity and documentation is built.

A clear purpose will help:

- identify what information you need to achieve the purpose
- determine which agencies should be involved
- help those agencies determine the best person to attend the meetings
- create transparency and help build public trust and confidence that you are sharing information appropriately.

Purpose of Sharing

Like your meeting purpose, having a clearly defined purpose (or purposes) for the sharing of information is critical. A clear purpose of sharing shows that the sharing is justified and carefully considered. It also helps stop 'scope creep' – that is, to stop the sharing changing over time without proper consideration or authorisation.

The purpose of sharing should be aligned with the purpose of the multi-agency meeting, for example:

Meeting Purpose	
To identify and implement appropriate supports for youth offending in specific areas.	
Purpose of Sharing	
Education	To determine whether attendance/lack of attendance at school is a contributing factor to offending; to identify appropriate attendance and engagement supports to reengage youth with education
Oranga Tamariki	To determine whether youth is currently under care and protection; identify existing services being provided; to identify appropriate care and protection supports for youth and their whanau
Police	To identify youth offenders; identify previous offending and interventions; identify appropriate interventions

Meeting Purpose	
To identify families affected by family harm and deliver a co-ordinated and consistent cross agency response	
Purpose of Sharing	
Education	To determine whether children and young persons identified as being involved in family harm are attending school regularly and where required identify appropriate supports for them and their whanau to engage with education
Oranga Tamariki	To determine whether child or young person identified as being involved in family harm are currently in care, or whether a care and protection intervention is required
Corrections	To determine whether a person involved in family harm is under the supervision of Corrections and whether any breach of conditions has occurred
Local Whare Maanaki	To enable Whare Maanaki to contact and engage with woman and children who have been identified as victims of family harm

Information to be shared

Through the development of your purpose statements (both the multi-agency meeting and information sharing purposes) you'll have determined:

- the information that needs to be shared to achieve those purposes, and
- the agencies that hold that information

You'll need to work with the attending agencies to identify the information they hold that is relevant to the purpose of your meeting. Attending agencies know their information holdings and understand any limitations on that information such as reliability, accuracy, and restrictions on secondary use.

Identify information relevant to your purpose

Identify this information early and record it in your multi-agency meeting protocol. This ensures that all attending agency representatives understand what information can be shared and for what purpose. It shows that you've carefully considered your information sharing and are only sharing what's relevant and appropriate. It will also help to identify the appropriate legal authority under which the information is being shared.

Skip to — Legal authority to share

Examples of identifying relevant information

Having this clarity on what's relevant enables timely information sharing and reduces unnecessary delays in achieving the purposes of the meeting — for example, identifying and providing appropriate support and services to individuals.

Attendance information held by Ministry of Education

Attendance information is made up of many attendance data variables, not all of which may be relevant to the purposes of a multi-agency meeting. The multi-agency meeting protocol should be clear on what attendance data variables are relevant to the purpose and will be shared at the multi-agency meeting.

Instead of recording 'attendance information' in the protocol, the protocol could record that the Ministry will share the attendance rate of the individual over the last X months, the number of justified and unjustified absences during the specified period, the reasons attributed to those absences, and any attendance interventions that have been put in place.

Health information held by Health NZ | Te Whatu Ora

Health information can be broad and in many cases sensitive. Not all health information will be relevant to the purpose of the multi-agency meeting. The multi-agency meeting protocol should be clear on what health information is relevant to the purpose and will be shared at the multi-agency meeting.

Instead of recording 'health information' in the protocol, the protocol should record the specific health information that Health New Zealand | Te Whatu Ora will share that is relevant for the purposes of the meeting. For example, where information is being shared to support reducing non-attendance rates, relevant health information could include current mental health diagnoses, disability information, and any health interventions/ supports currently being provided.

Identifying this information early and recording it in your multi-agency meeting protocol ensures that all attending agency representatives understand what information can be shared and for what purpose. It shows that you have carefully considered your information sharing and are only sharing what is relevant and appropriate. It will also help to identify the appropriate legal authority under which the information is being shared.

Having this clarity enables timely information sharing and reduces unnecessary delays in achieving the purpose(s) of the meeting, such as, identifying and providing appropriate support and services to individuals.

The multi-agency meeting protocol should clearly set out what information attending agency representatives can share, to whom, for what purpose.

Legal Authority to Share

There must be a legal authority to share information at multi-agency meetings. The multi-agency information sharing protocol does not itself provide the legal authority to share information. The multi-agency information sharing protocol must clearly state the legal authority for each of the purposes for which information is being shared.

Guidance on determining the appropriate legal authority - Legal authority to share information | NZ Digital government.

To help you complete your information sharing protocol we've included the common legal authorities used to share information in a multi-agency meeting. You can delete the legal authorities that do not apply to your multi-agency meeting, or manually enter the legal authority if it is not one of the examples provided for in the template.

Oranga Tamariki and Family Violence Acts

If you're using the Oranga Tamariki Act or the Family Violence Act information sharing provisions you'll need to ensure that attending agencies meet the criteria for sharing under those provisions.

Example 1 — section 66C of the Oranga Tamariki Act

Only the following agencies and individuals can share information using section 66C of the Oranga Tamariki Act:

- agencies meeting the definition of a child welfare and protection agency or
- a person meeting the definition of an independent person.

Example 2 — section 20 of the Family Violence Act

Only the following agencies or individuals can share information using section 20 of the Family Violence Act:

- agencies meeting the definition of a family violence agency or
- a person meeting the definition of a social services practitioner.

The multi-agency meeting protocol does not itself authorise the sharing of information – it cannot create or change the law.

All sharing of personal information must be permitted by legislation, such as the Privacy Act, the Oranga Tamariki Act, the Family Violence Act, or an agency's enabling legislation.

Use of information

Information shared at a multi-agency meeting must only be used for the specific purpose enabled by the legal authority. The purpose set out in the multi-agency meeting protocol needs to match what the legal authority allows.

Attending agencies should not put any information shared at a multi-agency meeting into their own business systems or records. An exception would be if they're doing so in order to carry out the specified purpose of that meeting.

That means you should not collect and store information about a person just because you think it might be relevant in the future. 'Just in case' is not a good enough reason.

Examples of use of information

Example 1 — Information sharing enabled by the Family Violence Act

The purpose of a multi-agency meeting is to identify family harm and provide support services and intervention to reduce the risk of family harm. If information is being shared to support that purpose then attending agencies can only use the information shared for one of the purposes described in section 20 of the Family Violence Act.

Example 2 — Integrating information into business systems

Information is being shared about a person for the purpose of providing support. An attending agency has no relevant supports or services to provide to that person at that time. Therefore the attending agency should not keep the shared information or add it to that person's file.

Things to note when keeping information

If the attending agency needs to keep the information so that it can carry out the purpose of the sharing, then it should note:

- where the information came from
- the legal authority the information was shared under
- for what purpose the information was shared
- any restrictions on what the information can be used for
- the date the information was shared.

Information Source	Legal Authority	Purpose	Date
Agency A	Family Violence Act, section 20	To complete a needs assessment and identify supports to reduce the risk of harm from family violence	1/7/2024

Secondary use of information

If at a later time an attending agency wants to use the information shared at the multi-agency meeting for a secondary purpose that agency will need to work through the purpose and legal authority assessments for the new proposed secondary use of the information.

Example 1 - Secondary use of information shared by attending agency

Police are called out to a family harm episode. The attending officers thought one of the persons present was under the influence of alcohol. The family harm risk was immediately addressed by a family member offering to take the individual to another location. All the parties present at the property were happy with this outcome. Police share the family harm report with Corrections in advance of the local family harm multi-agency meeting.

The supervising Probation Officer reads the report and identifies the individual as a person currently serving a community sentence. Given the circumstances of the family harm episode it appears that the individual has breached the conditions of their sentence. The supervising Probation officer shares this information with the Corrections representative who attends the family harm multi-agency meeting. The Corrections representative shares with the multi-agency meeting attending agencies that a potential breach of conditions has occurred. It is determined that specific information about the potential breach types will not be shared with the attending agencies as it is not relevant.

Can Corrections use the information from the family harm report to investigate whether enforcement action against the individual is required?

Yes, in this circumstance, they can. The Family Violence Act enables Corrections to use personal information shared at the family harm multi-agency meeting to make and carry out a plan that is related to, arises from, or responds to family violence.

In this case, the meeting participants can make a safety plan with Corrections being the lead agency in terms of carrying out the plan. The safety plan would include the individual's probation officer being advised of the family harm incident and engaging with the individual to identify whether there had been any high-risk situations over the last week. If it was determined through this engagement that a breach of conditions had occurred, appropriate enforcement action would be considered to help mitigate the risk of further family harm occurring.

Example 2 - Secondary use of information shared by attending agency

Ministry of Social Development (MSD) have a representative who sits on a local family harm SAM table. A family harm report is shared by Police. Attending agencies provide relevant information in relation to the individuals named in the report to assess the risks and needs of the individuals and contribute to a decision on appropriate supports for the whanau.

The MSD representative notices that the victim named in the report is a client. They also note that the report states the perpetrator of the harm is her partner who has been living at the address for 12 months. The client is receiving a solo benefit.

Can the MSD representative share this information with the fraud investigation team?

No, They can't. The information shared can only be used by the MSD representative for one of the purposes set out in section 20 of the Family Violence Act e.g. making or contributing to a safety assessment.

You should check with your privacy, legal or information sharing teams if you want to use the information shared at a multi-agency meeting for an unrelated secondary purpose.

Transparency and notification obligations

It's essential not to lose sight of the people behind the information that you are sharing.

Your multi-agency meeting information sharing protocol will already do this in a number of ways, for instance, by:

- having a clear and justified purpose
- using a legal authority that requires consultation (such as 66C of the Oranga Tamariki Act)
- limiting the information that is shared to what is genuinely necessary
- specifying controls that help to keep the information safe.

However, you should also set out the steps you'll take — also known as 'controls' — to make sure that people know about the information sharing. This is because, to the greatest extent possible, people should know which agency is collecting and using their information, and for what purpose.

It's hard to exercise their other rights without that knowledge. Sometimes, they may also be able to choose whether their information is shared or not.

Examples of transparency controls

Legal Authority	Example Transparency Controls
Oranga Tamariki Act (section 66C)	Prior to sharing any information about a child or young person an attending agency must, if it is practicable and appropriate to do so:
	1. inform the child or young person concerned or their representative about the proposed sharing including the purposes and likely recipients of any sharing
	2. provide the child or young person or their representative reasonable assistance to understand the information being shared, express their views about the proposed sharing, and understand any consequences resulting from the proposed sharing
	3. take into account the views expressed by the child or young person
	Attending agencies will meet the consultation requirements by
	• for example: only sharing information where consultation has occurred
	• for example: only share information with attending agencies where consultation has been attempted and has been unsuccessful
	• for example: confirm with SAM table facilitator that you have consulted with the child or young person prior to sharing information verbally at the SAM table meeting.
	OR
	Attending agencies consider that it is not practicable or appropriate to consult with the child or young person prior to sharing information at the multi-agency meeting for the following reasons:
	• for example: consulting with the child or young person prior to sharing their information could put the child at risk of further harm
	• for example: due to multiple agencies sharing information about the same child or young person at the same time resulting in multiple contacts from the attending agencies

Family Violence Act (section 20)	Attending agencies are not required to seek consent from, consult with or notify individuals when sharing and using information under section 20 of the Family Violence Act 2018.
	Where practicable and appropriate to do so, Police inform individuals (victim, perpetrator, or witness) at the time of attending a family harm incident that specified information about that individual will be shared with family violence agencies or social services practitioners for the purposes listed in section 20 of the Family Violence Act 2018.

Putting transparency controls into your multi-agency meeting protocol will help the attending agencies to be aware of and meet any obligations they may have to advise, notify, or consult people about the sharing of their information[1]. This is also a good place to note any controls that ensure that people will have an opportunity to have a say before any adverse actions are taken against them.

If there is a good reason not to tell people, modify the transparency clauses in the protocol template to be clear about what that reason is. Provide the clearest possible information without undermining the interests that you're protecting. For example, it may still be possible to reflect in am agency's privacy statement or transparency statement that the share happens, even though details are not given because it could undermine the ability to enforce the law.

Check with your privacy, legal or information sharing teams if you are unsure what your notification obligations are.

---

1   Including the proposed new IPP3A of the Privacy Act once it becomes law: Privacy Amendment Bill - https://www.legislation.govt.nz/bill/government/2023/0292/latest/whole.html

Method of sharing

You'll need to agree on the method of transfer of the information to the attending agency representatives. There are several ways information can be shared, including:

- the lead agency sends out a list of individuals that will be discussed at the meeting
- attending agency representatives share information verbally at the meeting
- attending agency representatives share information with each other via email prior to and/or after the meeting
- access to and use of a secure business system.

In all cases, attending agencies must ensure that the method of sharing information is one that's approved for use by their agency and protects the information.

Secure business systems and security classifications

Where a secure business system is used to share information, agencies must ensure that there's a robust policy about who can access the information so that it does not get accessed by people who do not have a legitimate reason to see it. Terms and conditions of use should also be clear.

If the information has been assigned a security classification, attending government agencies must ensure that the appropriate handling requirements under the Protective Security Requirements are met.

Skip to — Security Classification

If non-government organisations are attending the multi-agency meetings, ensure they're entitled to receive information with that security classification, and that they understand how to handle it.

Things to note about specific sharing methods

The following are some things to note when deciding how information to support the multi-agency meeting will be shared:

- The more sensitive the information, the more careful you will need to be when sharing the information. Think about:
  - Whether emailing the information is appropriate – do you need to password protect the sensitive information that is contained in an attachment? Should you share the information verbally at the meeting? Then follow up with a secure email to the relevant attending agencies after the meeting?

- If you are emailing information to attending agencies' representatives do you need to attach a security classification to the email, and can you use the SEEMail (or similar) functionality[2]?

- We recommend that you do not take hard copies of information to a multi-agency meeting as they're too easy to lose or leave somewhere where others can see them. However, if this cannot be avoided, ensure you:

    - keep the hard copy information secure at all times, especially if the meeting is held in a location outside your agency

    - securely destroy all hard copy information at the end of the meeting

    - do not provide the hard copy information to attending agency representatives unless it's appropriate and safe to do so.

- If you're attending a multi-agency meeting virtually, do not put personal information in the chat function. Doing so could make the information available to others, including to the software company. Also make sure that you cannot be overheard by people who're not entitled to know what happened at that meeting, for example if you're working from home.

- If the multi-agency meeting is supported by a business system (for example, the Family Safety System) or secure online collaboration space (for example, Microsoft Teams, CoLab), ensure you understand how the business system or collaboration space works. Do not share your access credentials with other people.

Any restrictions or controls that are put in place to ensure the method of sharing is secure should be recorded in your information sharing protocol. The protocol template provides some standard controls that you can use but you can also insert your own specific controls.

Check your agency's internal policies around the use of email and whether there are any processes you are required to follow when emailing personal information to external people.

---

2   Where the attending agencies are all government agencies compulsory use of SEEMail (or similar) functionality should be considered.

Security of the information

This section sets out the security controls required to protect personal information both during the sharing of the information and within the attending agencies own IT environment. The section contains two parts: security classification and security controls.

Security classification

Agencies must ensure that they comply with the New Zealand Government Security Classification Systems and Protective Security Requirements (PSR) when sharing information. The security classification will determine the additional controls required to protect the information and comply with the PSR. You'll need to identify the appropriate security classification and select from the drop-down box in the agreement template.

Protective Security Requirements — PSR Classification System

Your ICT or information security team should be able to help you identify the correct security classification for the information being shared.

As a general rule, all personal information should be classified as IN-CONFIDENCE at a minimum.

Security controls

Appropriate security controls are an important part of sharing personal information. A loss or compromise of information in transit or at rest can have serious impacts on people's privacy and on the agency's reputation.

The protocol template contains the minimum level of security controls that should be in place for all information sharing.

Depending on the nature of the information shared, you'll need to consider what additional security controls may be required and add these into the template.

Examples of security controls

Requirements

- Attending agency representatives have completed privacy and information security training modules — both internal modules and any modules associated with the use of a secure business system.

- All hard copy information shared at the meeting is securely destroyed at the end of the meeting.
- All email attachments containing personal information are password protected.

Restrictions

- Only sharing information with attending agencies from agency-approved devices.
- Not sharing personal information in the chat function, recording, or taking screenshots if the meeting is held virtually.
- Not sharing hard copies of information with other attending agency representatives.

Your ICT or information security team will be able to help you determine appropriate security controls to ensure the information is protected when it is shared with attending agencies.

Tikanga considerations

In many cases Māori data and information is a taonga and may require additional controls and restrictions to ensure the mana of the individuals is respected. Where you are proposing to share Māori data and information you should consider whether tikanga should be applied to the sharing and subsequent use of the data. This consideration is especially important when a Māori organisation or an iwi may be attending the meeting.

Tikanga is a set of values, principles, understandings, practices, norms and mechanisms from which a person or community can determine the correct action in te ao Māori[3]. Tikanga is not fixed. What tikanga will be appropriate will depend on the circumstances and should be determined through meaningful engagement with the people who may be impacted by the sharing and use of the information.

Each agency will have its own definition of Māori data, Māori Data Governance strategies[4] and Māori engagement practices that will guide considerations and incorporation of tikanga

---

3   E T Durie "Will the settlers settle? Cultural conciliation and law" (1996) 8 Otago Law Review 449 at 452. For academic writing on the definition of tikanga see Te Aka Matua o te Ture Law Commission The Taking into Account of Te Ao Māori in Relation to Reform of the Law of Succession (NZLC MP6, 1996); Moana Jackson "Where does sovereignty lie?" in Colin James (ed) Building the Constitution (Institute of Policy Studies, Wellington, 2000) at 196; Ani Mikaere "The Treaty of Waitangi and recognition of tikanga Māori" in Michael Belgrave, Merata Kawharu and David V Williams (eds) Waitangi Revisited: Perspectives on the Treaty of Waitangi (Oxford University Press, Auckland, 2005) 330; Robert Joseph "Recreating legal space for the first law of Aotearoa-New Zealand" (2009) 17 Waikato Law Review 74.

4   Māori Data Governance model – Te Kahui Raraunga: https://tengira.waikato.ac.nz/__data/assets/pdf_file/0008/973763/Maori_Data_Governance_Model.pdf

into any information sharing protocol. However, it's not up to the Crown to determine what tikanga applies. So, you should engage early with your Māori advisory teams to ensure engagement with Māori is undertaken appropriately and in line with agreed protocols and practices.

Retention and disposal of information shared

Attending agencies should only retain information shared at a multi-agency meeting if they're using that information for one of the meeting purposes — for example, undertaking a risk or needs assessment, identifying appropriate support services or interventions.

Where attending agencies do retain shared information for those purposes, they must ensure that the information is stored securely in their agency's approved business system. Once the information is securely stored in that business system you should securely delete any personal information that was shared using email.

Information shared under a multi-agency meeting information sharing protocol should only be held by an attending agency for the period for which the information is required. Attending agencies should understand their agency retention and disposal authorities and how they apply to the information being shared.

> You should also consider how the Lead attending agency will manage multi-agency meeting administration documentation such as meeting agendas, minutes and action logs.

Privacy and security breach management

It's important that the attending agencies know what to do if there is a privacy or security breach. Having this agreed in advance means you don't have to figure it out when a breach happens, and everyone is under pressure.

Identify:

- who should be told if there is a breach involving information shared at the meeting (pick an agency to be the contact point so everyone knows who to call. That agency will also be the one to contact the Privacy Commissioner if the breach is serious enough that they need to be notified).
- how the attending agencies will work together to help to respond to any breach (including deciding what to tell affected people

The protocol template provides standard clauses that cover the agencies' obligations in relation to privacy and security breaches. Check with your privacy team to make sure this fits with what's expected in your own agency.

Managing conflicts of interest

It is important that any conflict of interest is identified early and managed appropriately by both the lead agency and the attending agency representatives. Having a process for managing a conflict of interest helps attending agency representatives identify any conflicts early and know what they need to do to manage that conflict.

The protocol template provides standard clauses that set out how conflicts of interest should be managed in a multi-agency meeting setting.

Relationship management and oversight

Things change over time, so it's important to check periodically that the information sharing is working as expected and is still fit for purpose.

We recommend that each attending agency nominates a relationship manager. They will check how things are working and who's responsible for addressing any problems that arise.

They do not necessarily have to attend the multi-agency meetings, but they do need to have a good understanding of the meeting's purpose, which agencies attend, and what information is shared.

Relationship managers can also help support their agency representative with any information sharing issues that arise about their agency's information. This could include helping to liaise with the agency's privacy or legal teams.

We also recommend that relationship managers check in with the agency representatives on a regular basis to ensure that the protocol is operating as intended.

This helps to make sure any issues with the information sharing (such as scope creep) are picked up and fixed early.

Approving information sharing protocols

Agencies will have different approaches to who should sign a multi-agency meeting information sharing protocol. However, an information sharing protocol should be vetted by a person in a senior role related to privacy, legal or information and data, whether or not they are the person to sign the protocol themselves. This will make sure that the proper protections are in place, so attending agencies can be confident about their sharing.

It's important that the person approving the protocol has sufficient professional knowledge or has received specialist advice to be confident that it's appropriate to sign the protocol. This provides a level of integrity to the protocol and provides other attending agencies and the public with confidence that government agencies are sharing information appropriately.

Ultimately, each attending agency will need to determine the appropriate level of approval and sign-off for each information sharing protocol. However, the following are some helpful considerations:

Helpful considerations for information sharing protocol approvals

- Is it appropriate for attending agencies' representatives to sign the protocol on behalf of their agencies? Does this provide enough oversight of the protocol and assurance that the information sharing documented is appropriate?
- Senior level approvals and signoffs can take time – think about what parts of the protocol could be amended with agreement of another person (such as the Relationship Manager) rather than the original signatory
- How will you ensure that staff attending the meetings are aware of the protocol and understand how the protocol operates in practice?
- Should attending agency representatives have to acknowledge that they have read and understood the protocol prior to attending meetings?

Managing information sharing protocols

Oversight of information sharing protocols

It's important to have awareness and oversight of your information sharing protocol. You may need to:

- report to senior leadership on your information sharing activity
- respond to an Official Information Act (OIA) request
- know when to schedule resourcing for information sharing reviews
- know whether there is already a share in place — so you do not need to create another or so you can make quick changes to your existing sharing.

Having all your information sharing protocol information in one place creates efficiencies and supports good governance of your information sharing practices.

Each attending agency should be provided with the completed and signed protocol so they can add the protocol to existing information sharing catalogues or registers.

Review contents and processes

Reviewing your multi-agency meeting information sharing protocol ensures that your information sharing remains fit for purpose. It ensures you're still only sharing information necessary to achieve the purposes of the meeting.

You may find that additional information held by non-attending agencies is required to achieve the meeting purposes. Or, that different methods are required to share the information more securely. Reviewing the protocol will identify these new requirements and processes and enable the protocol to be amended and updated in a considered way.

The protocol template includes a section for stating an appropriate review period, and which attending agency is responsible for initiating the review.

If the multi-agency meeting has a lead agency, it's recommended that that agency initiates and manages the review. There should also be a process for an attending agency to request a review of the protocol at any time if an issue with the sharing of information has arisen.

Steps for reviewing an information sharing protocol

A review of the multi-agency meeting information sharing protocol should involve the following steps:

1. A thorough read through of the document
2. Contact with the other attending agencies to confirm whether:
   - The information sharing as documented is still required
   - There have been any material changes to the purposes for which the information is being shared
   - There have been any material changes to the use of the information shared
   - Any issues have arisen with the quality of the information shared
3. Work with the other attending agencies to make the necessary amendments to the protocol
4. Sign off the amendments and update the protocol
5. Provide a copy of the signed updated protocol to all attending agencies
6. Ensure all attending agency representatives are aware of the changes and understand what those changes mean for them.
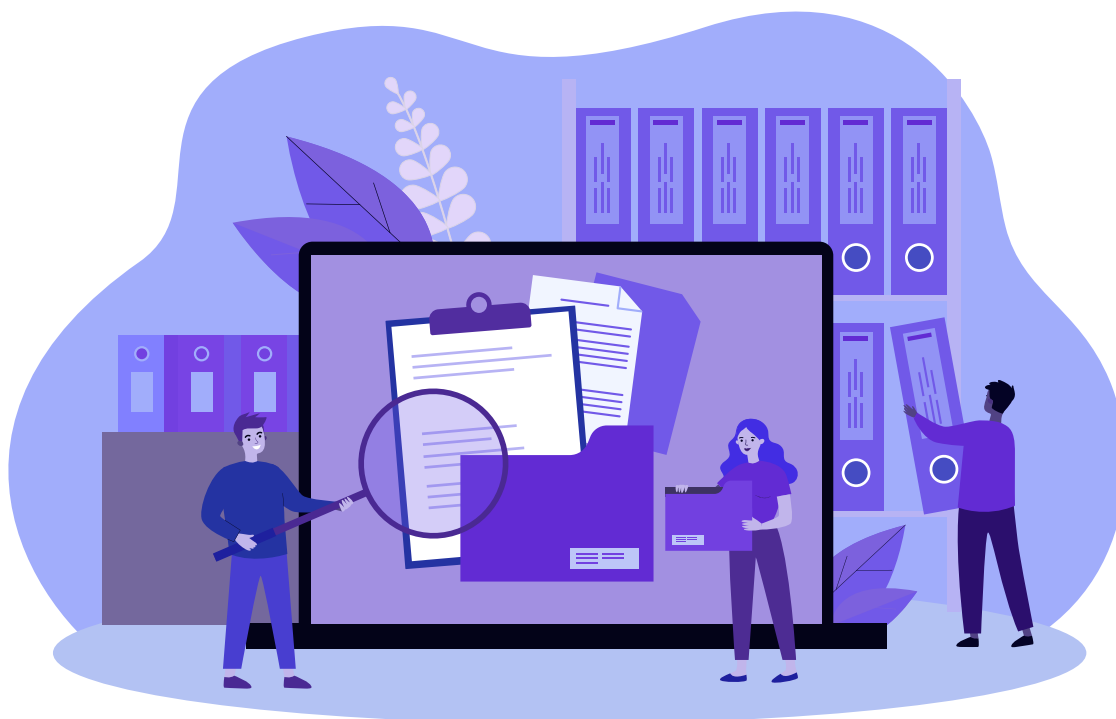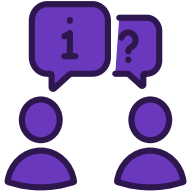
Information for people attending a multi-agency meeting

If you have been invited to attend a multi-agency meeting there are a number of things to think about before attending.

Use this checklist to help you prepare and give you confidence around:

- what information you can share
- with whom and for what purpose
- the legal authority under which you'll be sharing the information.

Who should attend?

To ensure the multi-agency meeting is productive and the right information can be shared with the right people, the right people need to attend.

Think about the following:

- Are you the right person to attend the meeting?
- Is your role one where you have access to the information that might need to be shared (either at the meeting or prior to or after the meeting)?
- Do you have sufficient knowledge about the supports and interventions that your agency can provide?
- Do you have any conflict of interest (perceived or actual) that may impact your ability to participate the meetings?

What information can I share?

You should only share information that is relevant to the purposes of the multi-agency meeting.

- Ask for a copy of the information sharing protocol - it is important that you are aware of this protocol and understand what information you can share and for what purpose.
- Ensure you are familiar with the legal authority under which you are sharing and using information. This will give you confidence that you are sharing information appropriately and help you navigate any judgement calls you may have to make about whether certain information should be shared or not.
- Understand whether there are any limitations or restrictions on the information you are sharing – is the information up to date and accurate, does the information have a security classification that requires additional handling requirements, is the information subject to any tikanga, does the information have a legal definition that the other attending agencies should be aware of?

If you are in any doubt about whether personal information can or should be shared at a multi-agency meeting check with your privacy, information sharing or legal team.

What information can I use?

You should only use information shared at a multi-agency meeting for the purposes set out in the multi-agency meeting information sharing protocol.

- Again, this should be clear from the information sharing protocol.
- When information is shared with you at a multi-agency meeting, make sure you understand why the information is being shared with you, and what you are allowed to do with it.
- If the multi-agency meeting is one where attending agencies are tasked to undertake certain actions (for example, to contact a named person to undertake a welfare check), ensure you only use the shared information for that purpose.

How do I share information with the members of the meeting?

It is important that you share information with other attending agencies in a secure manner.

- Ask for a copy of the information sharing protocol – it is important that you know how information has agreed to be shared securely with other attending agencies.

- If information is to be shared using email:
  - understand your agency's policies around emailing personal information to external parties.
  - think about whether emailing the information is appropriate in the circumstances – do you need to password protect more sensitive information in an attachment, should you verbally share the information at the meeting, then follow up with a secure email to the relevant attending agencies after the meeting?
  - do you need to attach a security classification to your email? Does the recipient/s of the email have the necessary security clearance to receive the information within your email?
  - are you required to use SEEMail (or similar) functionality? If so, do you know how to use SEEMail (or similar) functionality?

- We recommend that you do not take hard copies of information to a multi-agency meeting. However, if this cannot be avoided ensure you:
  - keep the hard copy information secure at all times, especially if the meeting is held in a location outside of your agency
  - securely destroy all hard copy information at the end of the meeting
  - do not provide the hard copy information to attending agency representatives

- If you attending a multi-agency meeting virtually do not put personal information in the chat function, do not record the meeting, and do not take screenshots of information shared using the share screen functionality.
- If the multi-agency meeting is supported by a business system (e.g., the Family Safety System) or secure online collaboration space (e.g., Microsoft Teams, Colab), ensure you understand how the business system or collaboration space works and do not share your access credentials with other people.

Before you share information at a multi-agency meeting check your agency's policies and requirements for emailing personal information to external parties.

How do I manage a conflict of interest?

If you attend a multi-agency meeting and information is being requested and shared about a person you know this may create a conflict of interest for you. If this occurs you should:

- inform the multi-agency meeting facilitator as soon as you become aware of the conflict of interest
- refer the request for information to another person within your agency to action and respond to
- remove yourself from the meeting when information is being shared about the individual that creates the conflict of interest

Can I share information about the interventions or supports my agency has provided?

Where your agency has been tasked with using the information shared at a multi-agency meeting to undertake an action enabled by the legal authority (for example a risk or needs assessment or provide a support service) you can share with the attending agencies the outcome of that action.

Where the multi-agency meeting uses a business system to manage the sharing of information and tasking of actions, you can enter the outcome of your tasking activity directly into the business system (for example, the outcome of a safety risk assessment undertaken by an agency in response to a family harm incident can be entered directly into the Family Safety System).

Glossary

This section sets out the meaning of key terms used within the guidance.

Agency

Includes government agencies and departments, departmental agencies, and non-government organisations

Attending Agencies

Agencies that attend the multi-agency meeting and are signatories to the multi-agency meeting information sharing protocol

Lead Attending Agency

The attending agency that sets up the multi-agency meeting and is responsible for developing and implementing the multi-agency meeting information sharing protocol

Information

Includes data, personal information, aggregate information, and de-identified information.

Māori Data

Digital or digitisable data, information, or knowledge (including matauranga Māori) that is about, from or connected to Māori. It includes data and information about population, place, culture, and environment[5].

Multi-Agency Meeting

A meeting where different agencies and organisations come together for a common purpose in a meeting setting. These meetings can be one-off events or occur regularly over a period of time

Organisations

Non-government entities, or groups.

---

5   Te Kāhui Raraunga, 2021a; Te Mana Raraunga, (2018)

Appendix One: Multi-agency meeting information sharing protocol template

A copy of the protocol templates can be downloaded here:

[Link to multi-agency meeting information sharing protocol template](#)