Sharing information safely

Guidance on sharing personal information under the Family Violence Act 2018

New Zealand Government

Foreword

New Zealand Government

Ministry of Justice
Tāhū o te Ture
justice.govt.nz
ISBN 978-0-478-32481-5
June 2019

This Guidance may be revised periodically.
Make sure you are working with the most current version.

Images used throughout this document are intended to illustrate providers networking and are from a photolibrary using models.

Foreword

New Zealand has unacceptable rates of family violence, which severely undermine the lifetime wellbeing of victims and their children. Violence affects New Zealanders across all socio-economic and cultural groups, reflecting and reproducing the inequalities across our communities. Eliminating family violence is one of our greatest opportunities to improve the wellbeing of New Zealanders.

An integrated and responsive system requires agencies to understand their role, collaborate, share information and invest in the workforce that supports people affected by violence. All of us have a part to play in ending family violence. We need action across Government and in all communities.

The Ministry of Justice received substantive, meaningful feedback from the family violence sector throughout the development of the Guidance, including victims of family violence, non-governmental organisations, community leaders, iwi representatives, individual practitioners and government agencies. I very much appreciate the effort and commitment of everyone who is contributing to this crucial work.

This Guidance provides practical help for everyday work in the family violence sector, including basic diagrams, explanations and case examples to help illustrate what to do when you want to share information. It is designed to serve as a tool to support the sector in delivering consistent and effective services to respond to family violence.

I acknowledge the complexity of the issues; there is no quick fix, but change is possible, and this Government is determined to make progress. People should have confidence in the family violence and sexual violence response systems – to keep people safe, ensure victims are heard and enable behaviour change. Enabling the safety and wellbeing of our families and whānau requires action across Government and in all communities. Everyone has a part to play.

Together we are stronger.

Jan Logie MP

Parliamentary Under-Secretary to the Minister of Justice
(Domestic and Sexual Violence Issues)

CONTENTS

Please note: Case examples used throughout this Guidance are for explanatory purposes only. The scenarios described are fictitious, and are not intended to reflect the complexities of family violence situations. They should be used as high-level practical guides, and any resemblance to actual persons or scenarios is coincidental.

PART I

Key information

A. What is the purpose of this document?

The Family Violence Act 2018 (the Act) came into force on 1 July 2019. The Act introduced rules about when personal information can be shared, to encourage the sector to collaborate and respond to family violence. Under the new laws, you **must consider sharing information** if you receive a request from another agency or practitioner in the sector, or if you believe that it may protect a victim from family violence. Sharing information is not mandatory and will require you to think about what might be relevant to share to achieve one of the specified purposes.

Safe and appropriate information sharing within the sector has benefits for victims and assists frontline staff to mitigate the risk of harm and address the effects of family violence. It's important to follow the steps in this Guidance and use your professional judgement when sharing information to make sure you're not putting a victim or others at risk of harm.

The new information sharing provisions in the Act are designed to:

- protect people from family violence and make it easier for them to get help
- ensure information sharing occurs in a way that is safe
- encourage the sector to share personal information about clients and work collaboratively to respond to family violence
- provide the sector with certainty and confidence that the law will protect them when sharing information appropriately.

This Guidance is to assist **family violence agencies** and **social service practitioners** to apply and use the new information sharing provisions under the Act. It provides practical help for everyday work in the family violence sector, and includes a decision tree poster on page 8 that takes you through the things you should think about when sharing information. You can print this poster out for easy use when making information sharing decisions.

Remember that behind every piece of personal information there's a real person, who deserves respect and dignity. The person whose information you hold should be kept in the front of your mind at all stages of the information sharing process. Their personal information does not belong to you – you are a **kaitiaki, a custodian, of the information**.

Family violence is defined in section 9 of the Act. Family violence can include physical abuse, sexual abuse or psychological abuse, and may present as a pattern of those types of behaviours. Often, that pattern features actions done with the aim of coercing or controlling the victim. Coercive or controlling behaviour includes actions which make the victim dependent on the perpetrator or isolate the victim from their friends or family. It often causes cumulative harm that may not be apparent from any one incident viewed in isolation.

It's important to recognise that someone you may be working with could be experiencing coercive or controlling behaviour. Sometimes this might mean it's difficult for victims to come forward or ask for help. When you are working with victims of family violence it's important to understand these dynamics and the effect they might have on the victim's ability to respond to the situation. Information sharing, and ensuring the victim is involved in the process, is one way we can ensure better responses to family violence.

This Guidance sits alongside the *Risk Assessment and Management Framework* and the *Workforce Capability Framework* as a tool to support the sector in delivering consistent and effective services to respond to family violence. If you're not familiar with family violence dynamics or risk, you should take some time to familiarise yourself with these documents. You can find the frameworks here: **www.justice.govt.nz/justice-sector-policy/key-initiatives/reducing-family-and-sexual-violence/work-programme/**

If you wish to read the Act in full you can find it on the New Zealand Legislation website, at: **www.legislation.govt.nz**. For a list of terms used in this Guidance, see Appendix 1.

B. Who does this Guidance apply to?

There are two groups of people who can share under the Act and use this Guidance: **family violence agencies** and **social services practitioners**. Some people you work with may not be covered by the Guidance – see Appendix 2 for more information.

(a) Family violence agencies

Family violence agencies are defined to include:

- specified government agencies
- non-government organisations ('NGOs') that are partly or wholly funded by government to deliver family violence services
- school boards and licensed early childhood services (as defined in the Education Act 1989).

The specified government agencies are:

- the Accident Compensation Corporation
- Department of Corrections
- Ministry of Education
- Ministry of Health
- Ministry of Justice
- Ministry of Social Development
- Oranga Tamariki – Ministry for Children
- New Zealand Police
- Immigration New Zealand
- District Health Boards
- Housing New Zealand Corporation, and
- registered community housing providers.

(b) Social services practitioners

Social services practitioners are defined as individuals who are providing education, health or other social services. This includes:

- teachers with current practising certificates or limited authority to teach
- registered health professionals (including, but not limited to, general practitioners, midwives, nurses, and psychologists), and
- registered social workers.

*This Guidance collectively refers to these agencies and individuals as **"the sector"**.*

C. How does this Guidance interact with other information sharing resources?

The Oranga Tamariki Act 1989 and the Family Violence Act work together to regulate how people's personal information can be shared in certain situations. The legislative requirements under these Acts are similar in many ways, but there are some key differences including who the requirements apply to, and the purposes that information can be shared for.

The four most important things to know about how the Acts work together to support good information sharing are:

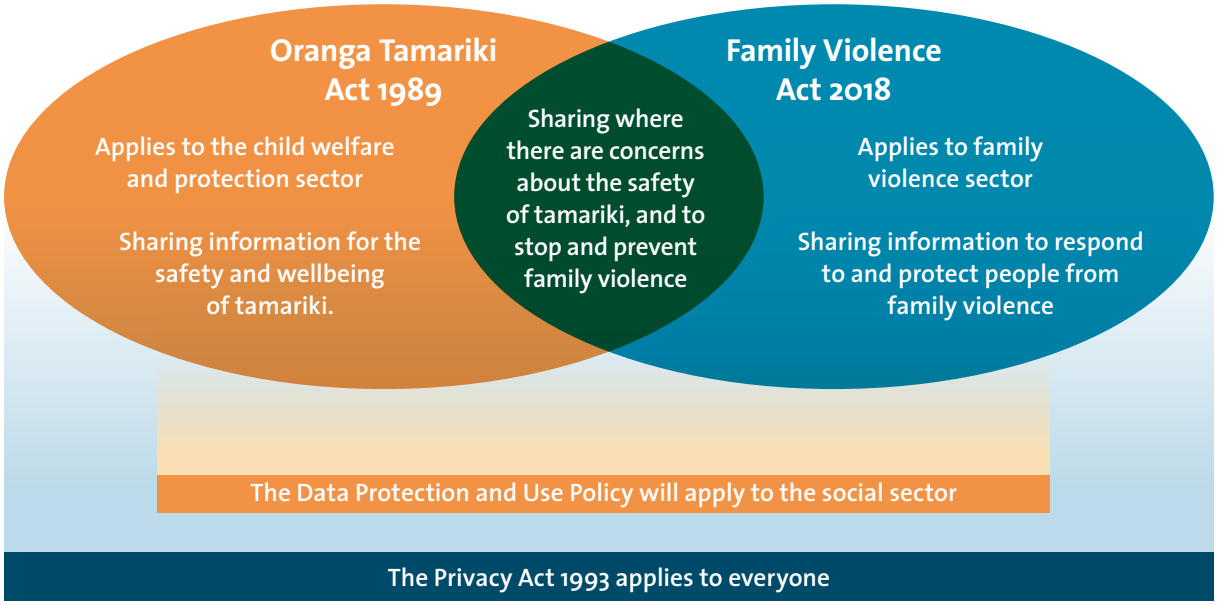
1. **Safety comes first** – personal information should be shared with the right agencies or practitioners if there are concerns about someone's safety or they or others are at risk of harm. The Oranga Tamariki Act and Family Violence Act override the limits on disclosure of personal information set out in the Privacy Act 1993 so that you can share information in more situations to keep people, including tamariki, safe.
2. **Professionals can proactively share information, but in most cases it's not compulsory** – professionals and agencies should feel confident and empowered to proactively share information when it fits with the purposes of either Act. However, it's important to remember there are no mandatory or compulsory information sharing requirements across the social sector (except when Oranga Tamariki or the Police make a request under section 66 of the Oranga Tamariki Act).

> Remember that behind every piece of personal information there's a real person, who deserves respect and dignity.

3. **You are protected when you share in good faith** – If you share information in good faith, and comply with the information sharing provisions in the Acts, you are protected from civil, criminal or disciplinary proceedings.
4. **The Oranga Tamariki Act and the Family Violence Act go beyond the Privacy Act in some circumstances, but other parts of the Privacy Act still apply** – the Privacy Act has twelve principles that agencies must follow when collecting, storing, using or disclosing personal information. While any sharing of information under the Oranga Tamariki Act or Family Violence Act overrides the limits on disclosure of personal information, the other requirements in the Privacy Act (such as storage) still apply.

D. How can I provide feedback?

Like the family violence system itself, this Guidance needs to evolve to reflect best practice and adapt to the changing needs of the workforce. There will be opportunities to update the Guidance in the future to ensure it continues to support the family violence sector. If you have any comments, suggestions or ideas for improving this Guidance please contact: FVinformationsharing@justice.govt.nz.



The Privacy Act controls what and how agencies collect, use, disclose, store, and give access to information that identifies an individual. You can find out more about the Privacy Act on the Privacy Commissioner's website: www.privacy.org.nz/the-privacy-act-and-codes/the-privacy-act/

The Data Protection and Use Policy (DPUP) will set out expectations of the values and behaviours that promote the safe, transparent and ethical collection, use, and sharing of identifiable, aggregate and de-identified data and information across the social sector. While DPUP will not be legislated, following DPUP will be a great way to build New Zealanders' trust in how their data and information is being used, and ensure transparency.

DPUP is currently in a draft format and is expected to be published mid to late 2019. You can find out more about DPUP on the Social Investment Agency's website: www.sia.govt.nz/investing-for-social-wellbeing/data-protection-and-use/

PART II

Sharing information

Principles of family violence information sharing

This Guidance is based on eight principles that highlight the key parts of information sharing under the Act. You can use these principles and the decision tree poster on pg. 8 to guide you through the information sharing process:

1	People's safety comes first
2	You should obtain consent to share information when it is safe to do so
3	You must consider sharing information if you think it will protect a victim or if you receive a request
4	You can share information for specific purposes
5	You must only share relevant information
6	You should check that the information is accurate
7	You should record reasons for your decisions
8	You have legal protection from liability when you share information, unless you share in bad faith

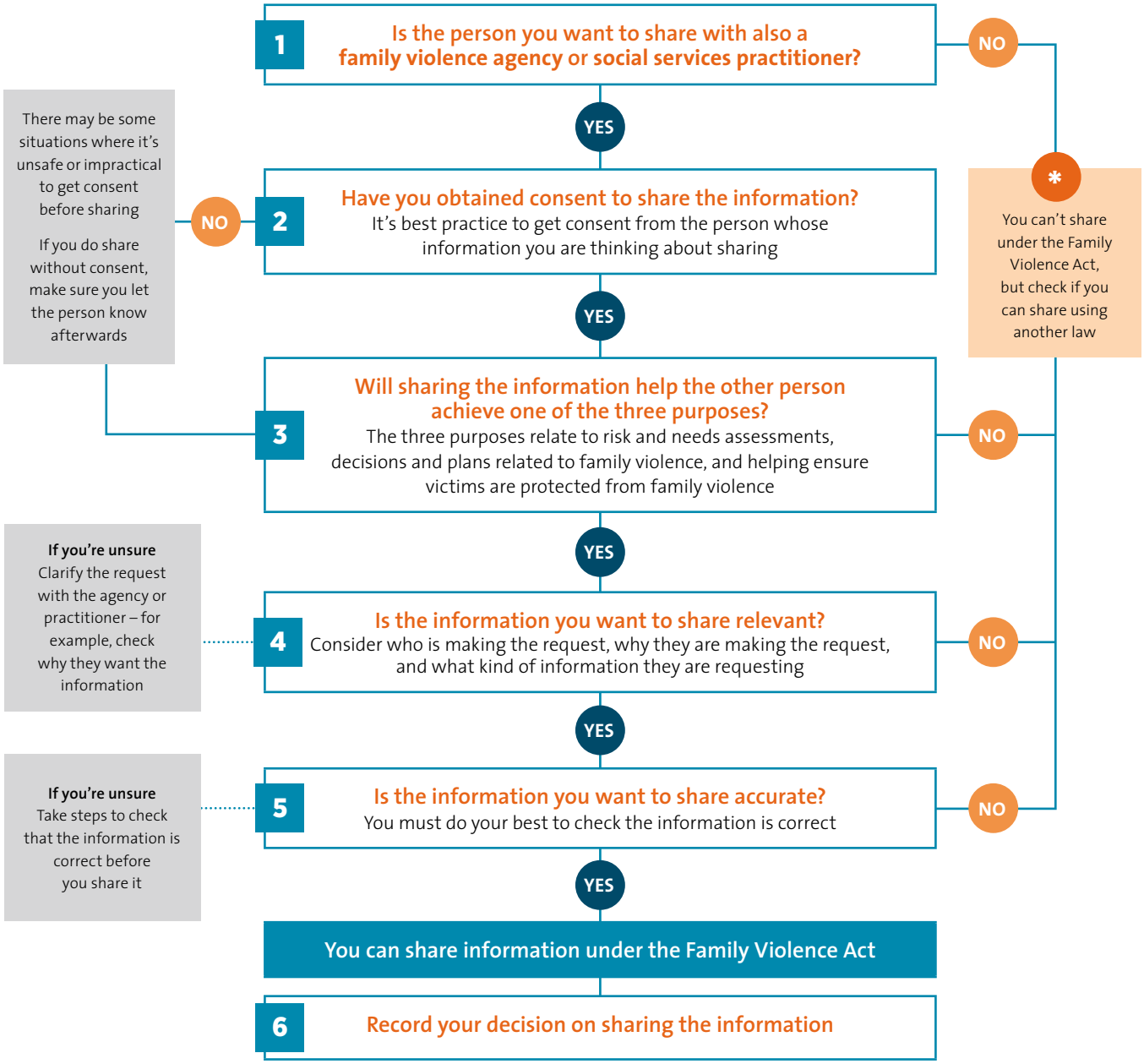
Guide to sharing information

Under the Family Violence Act 2018

REMEMBER: You have a duty to consider sharing information if:

- you get a request from another agency or practitioner, OR
- sharing may help protect a victim from family violence.

See Principle 3 in the Guidance for more information



Family violence agencies include:

Specified government agencies

ACC | Corrections | Ministries of Education, Health, Justice, Social Development | Oranga Tamariki | Police | Immigration NZ | District Health Boards | Housing NZ | Registered community housing providers

Non-governmental organisations that are partly or wholly funded by government to provide family violence services

School boards and **licensed early childhood services**

Social services practitioners include:

Teachers with practising certificates or limited authority to teach

Registered health practitioners

Chiropractors | Dietitians | Medical radiation technologists | Doctors | Medical laboratory science professionals | Anaesthetists | Nurses | Occupational therapists | Optometrists | Physiotherapists | Podiatrists | Psychologists

Registered social workers

Guide to sharing information Under the Family Violence Act 2018

Better collaboration and coordination through information sharing can help protect people from family violence and make it easier for them to get help. If you meet the requirements in the Guidance and follow the steps set out in the decision tree, you can share under the Family Violence Act.

You have a legal duty to consider information sharing if you receive a request, or if you think sharing may help protect a victim from family violence. This duty doesn't stop you from sharing information in other situations, so long as the sharing is for one of the specified purposes.

1

You can share information with another agency or practitioner who is covered by the Family Violence Act

Being a family violence agency or social services practitioner means you're allowed to share information with other family violence agencies and social services practitioners, so long as you also meet the Family Violence Act's other requirements. This means you and others can more effectively assess and manage family violence risk. If you receive a request from someone and you're not sure who they are or whether they are covered, you should make reasonable enquiries to check.

More information on family violence agencies and social services practitioners covered by the Act can be found on page 5 of the Guidance.

2

You should try to get a person's consent before sharing their information

It is best practice to get consent from the person you are sharing information about, unless it is unsafe or impractical to do so. You should explain to the person what information you want to share, who you want to share it with and why. Remember that the information is someone's life and story, and that losing control of that information can cause harm.

There may be some cases where you will be required to make a judgement call on whether you should share information without someone's consent – for example, if you are concerned for someone's immediate safety.

If you are not able to get someone's consent before you share their information, you should take steps to let them know you shared their information afterward, if it is safe to do so (e.g. you are not putting yourself or others at risk).

More information on obtaining consent can be found in Principle 2 of the Guidance.

3

You must reasonably believe that sharing the information could help the other person achieve one of the purposes

To share under the Family Violence Act, you must believe that your sharing will help the other agency or practitioner achieve one of the following purposes:

- to help ensure that a victim is protected from family violence
- to make or contribute to a family violence risk or needs assessment
- to make, or contribute to the making or carrying out of, a decision or plan relating or responding to family violence.

If you don't think sharing will help the person achieve one of the purposes, then you cannot share the information under the Family Violence Act. You can check whether you can share the information under another law.

More information on the purposes for sharing information can be found in Principle 4 of the Guidance.

4

You must only share information that is relevant

When you are sharing information with another agency or practitioner, you should only share information that is relevant. Relevance will depend on the circumstances, including the role of the other person and what purpose they want to use it for. Think about who is making the request, why they are making the request, and what kind of information they are requesting.

You must make a judgement call on whether the information you hold is relevant to the person you want to share it with. For example, information about a child being absent from school may not be relevant to share with a doctor, while information about a person's health may not be relevant to share with some government agencies. If you share information that is irrelevant, you may be acting in bad faith and may not be able to rely on the legal protection under the Family Violence Act.

More information on the relevance of information can be found in Principle 5 of the Guidance.

5

You must check that the information you are sharing is accurate

Under the Privacy Act 1993, you must take reasonable steps to ensure information is accurate, up-to-date, relevant and not misleading. This requirement applies to information you share under the Family Violence Act. You should take steps to make sure the information you share is correct.

There may be situations where you have a hunch or suspicion that you want to share, but you are not sure you are right. You're allowed to share your suspicions, so long as you let the other person know it is merely a suspicion and not a fact.

More information on the accuracy of information can be found in Principle 6 of the Guidance.

6

You should record your decision to share the information

Keeping records of requests for information, including details of the request, your response to the request, and whether or not you obtained consent to share, is good practice. You should also make sure you record situations where you decided not to share.

If you are asked questions about the situation in the future, good record-keeping will mean you can answer confidently and provide evidence in support of your decision. It also means you will have the information you provided ready if you receive another request for the same information.

More information on recording your decision-making can be found in Principle 7 of the Guidance.

*****

If you can't share information under the Family Violence Act, you might be able to under another law

The Family Violence Act only allows information to be shared between specific people, in specific circumstances. If you don't meet the requirements to share under the Family Violence Act, but you think it's important that you do share the information, you might be able to do so under another law.

You should check other laws and guidance to see if they might apply in your situation, including:

- Privacy Act 1993
- Oranga Tamariki Act 1989 and related information sharing guidelines
- Health Information Privacy Code 1994

PRINCIPLE ONE

People's safety comes first

Information sharing that is done safely, appropriately and consistently, can help **ensure a victim's safety**. Sharing information means that agencies are able to effectively assess and manage risk, and coordinate appropriate responses.

The law makes it clear that people's safety should always come first, and that sometimes this will mean sharing someone's personal information to respond to family violence. If you can't keep someone safe from harm and protect someone's confidentiality at the same time, then safety takes priority.

You need to make sure that the information you share, who you share it with, and the way in which you share it is appropriate, and that you **don't expose the victim or others, including children, to greater harm**. Victims are experts of their own experiences and needs, and often will know what will help to keep them safe. There are likely to be safer outcomes when the victim is involved in the information sharing process.

It's important to recognise that sharing information can sometimes make people **less safe**. For example, if a victim's information ends up in the hands of a perpetrator it could then be used to contact the victim, or as a tool to harass the victim. The sensitivity of personal information – that is, the harm that it might do in the wrong hands – will vary depending on the circumstances. For many people, contact details are relatively public and they are not concerned if those details are shared. For a victim of family violence, however, contact details may be among the most sensitive information that they provide.

It's also important to remember the way you record information may cause harm if it's inaccurate or based on unsubstantiated claims. Once information is on file, it often becomes the accepted version of events. **Take care to record things factually** and, if you're not sure if something is correct, check with the person whose information it is. For more on ensuring information is accurate, see Principle 6.

Information must not be shared:

- if it would make the victim or others (such as children) unsafe, and
- it is not possible to mitigate those safety risks by sharing information in a particular way or with particular conditions attached.

Before sharing information, you should carefully consider whether sharing could create or worsen safety risks for victims. It's not just a question of whether information should be shared at all – it's also a question of how or when it's shared. There may be alternative ways you can share information to avoid safety risks.

> ***For example,*** *the victim may know that a member of the perpetrator's family or whānau works at a community organisation. They might have concerns that being referred there will make them unsafe. Once you understand the situation, you can send them somewhere else and avoid the problem.*
>
> *Or, if there's no other provider, you may be able to negotiate an alternative process to keep the victim safe. Keep the victim informed. They may then be willing and feel safe to use the service.*

Talk to the victim to find out whether it is safe to share particular information with a specific agency. They are likely to have the best understanding of risk and what actions are likely to increase or decrease that risk. Talking to the victim may alert you to risks that you are unaware of, or they may be able to suggest that you share information in a way that will achieve the same results for them, but in a safer way. You can also use that opportunity to check with the person that the information you are wanting to share is correct.

The *Risk Assessment Management Framework* sets out a common approach to screening, assessing and managing family violence risk. You can access the Framework and find more information on risk factors and the dynamics of family violence here: **www.justice.govt.nz/justice-sector-policy/key-initiatives/reducing-family-and-sexual-violence/work-programme/risk-assessment-management-framework/**.

CASE EXAMPLE

Sharing information to protect someone's safety

Carmen is a social worker in a small town. She is approached by Maria, who has been being increasingly isolated and abused by her partner Greg for some time. Carmen believes the abuse is escalating and that Greg may seriously injure or kill Maria.

Maria is very reluctant to lay charges with Police as she is fearful of retribution from Greg if she does. However, Maria is on a community-based sentence and consents to Carmen sharing information with her Probation Officer, Sam, who is employed by the Department of Corrections. Maria, Carmen and Sam meet and discuss Maria's risk of serious harm. At that meeting Maria reinforces that she does not consent to Police being involved.

Following the meeting, Carmen and Sam suspect that Greg's controlling behaviour is influencing Maria's reluctance to tell Police. They decide to share Maria's information with Police as they are genuinely concerned that Maria will be seriously harmed and they know Police can help protect her. They tell Police that Maria does not consent to this disclosure. Afterwards, they both keep a record of what information they shared, that the information was shared without consent, who they shared it with, and why.

Carmen informs Maria that she has shared the information with Police, and works with Maria to develop a plan to keep her safe. Carmen also lets Maria know of other support services she can access, and helps her to reach out to them.

PRINCIPLE TWO

You should obtain consent to share information when it is safe to do so

It is always **best practice to seek the person's consent before sharing their information**, unless it's unsafe or impractical to do so. Inconvenience is not enough – there must be genuine obstructions to gaining consent. For example, if the person does not respond to repeated attempts to contact them, or if immediate action is required to keep someone safe. Consider what efforts you would expect someone to make before sharing information about you.

Getting a person's consent before sharing their information is an important way of involving them in the process and upholding their autonomy and mana. Conversations about consent can alert you to safety risks that you might not have otherwise thought about, and allows you to check whether the information you hold is correct.

However, the Act **does not require** you to get a person's consent before you share their personal information. The law makes it clear that keeping people safe always comes first. Sometimes this means you may need to share personal information without getting the person's consent so that you can protect them or others. This should be the exception, and not the general rule.

If, despite your best efforts, you can't obtain consent before sharing information, you should take steps to **let the person know** as soon as possible afterward if you can do so safely. Maintaining a transparent and trusting relationship with your clients is important. Where a client has been involved in decision-making they may be more willing to access and engage with support.

"Consent" needs to be genuine and informed – that is, the person needs to know what they are agreeing to. Informed consent means letting the person know:

- what information will be shared
- with whom
- for what purposes, and
- what the consequences of that information sharing might be (particularly if there could be any negative consequences for them).

It's vital that people feel safe seeking help. Victims need to be able to trust that you'll manage their information properly, share information appropriately, and not expose them to more risk. Remember that different cultures may have different views on what privacy and consent mean – you may need to tailor your approach depending on who you're working with.

A. What if I can't get consent?

There may be situations where it's not safe or practical to get a person's consent before sharing their information. For example, where:

- you are not able to get in contact with the person, despite making reasonable attempts to do so
- discussing the situation with the person or trying to get their agreement would create additional serious safety risks, or exacerbate existing risks
- you need to share information quickly so you can assess the risk of harm and address the harm promptly
- discussing the situation could jeopardise a Police investigation or a prosecution, or
- it is not possible to contact the person safely or at all.

Think about the surrounding circumstances and use your judgement. Seeking and obtaining consent helps engage the person in the process and is always best practice. While information sharing can relieve people of the responsibility to make all the arrangements to resolve their situation, it should not be used as an excuse to override people's autonomy, except in circumstances where this is clearly justified.

B. When should I tell a person that I have shared their information?

If you have shared a person's information without getting their consent, you should **let them know** afterwards, if it is safe and appropriate. You should tell the person what information was shared, who it went to, and why you shared it. You can also let them know about their rights in regard to that information – for example, that they can request to see and correct the information. See Part III: Collecting, storing and keeping information for more information.

In some cases, it may not be appropriate to tell someone you have shared their information, for example, where it could put them or others in danger. Again, it is best practice to let the person know to involve them in the process - use your professional judgement to make a decision.

C. Who can I share with if I do have consent?

The Act only allows personal information to be shared for specific purposes (see Principle 4 for more information). However, if a person has given you their informed consent, you are able to share any of their information to the extent that they have agreed, even if it doesn't fall within one of the specified purposes. You can have a conversation with the person about who should have the information about their family violence situation, and why that might help them.

You may like to discuss sharing their information with not only other agencies and practitioners, but also whānau. Whānau or family members can be especially important in providing assistance to people affected by family violence. They are often the people closest to the victims or perpetrators and can be best placed to provide ongoing support.

If a person **does not consent** to you sharing information with someone who is not covered by the Act, you can't share with them under this law. Check to see if any other laws apply – remember that you can always share to protect someone from a serious safety threat.

CASE EXAMPLE

Sharing with consent

Li Mei is an ACC case manager and is concerned about one of her clients, Tīhema. Tīhema has had several claims for injuries that are consistent with family violence. Li Mei wants to share this information with Miriama, a support worker at a family violence service provider that Li Mei has worked with for several years.

Li Mei asks Tīhema for his consent to share information about his injuries with Miriama. She also checks that the information she has about Tīhema is correct. Tīhema lets Li Mei know that he has moved recently and provides his new address. He then consents to Li Mei sharing his information. Li Mei shares the information, then records what she shared with Miriama, why she shared it, and that Tīhema consented to the information being shared.

PRINCIPLE THREE

You must consider sharing information if you think it will protect a victim or if you receive a request

The Act introduces a new duty on the family violence sector. It says **you must consider sharing information** where you reasonably believe that it may protect a victim from family violence, or where you receive a request from another agency or practitioner in the sector. The duty to consider only applies in these two circumstances, however, it does not prevent you from sharing relevant information in other situations for a specified purpose.

You must consider sharing information even if:

- the personal information is confidential, or
- the person concerned has not given their consent to the information being shared.

The duty requires you to **think about sharing** information, but it does not force you to share. If you decide not to share information, even though one of the specified purposes applies, keep a note of why you made that decision. For more information about record-keeping, see Principle 7 of this Guidance.

A. Why is there a duty to consider sharing?

We need a more effective and integrated system to reduce the risks of family violence. We also need to make it **easier for people to get help** and keep people safe. Sharing information is one way we can do this.

A formal duty to consider sharing was created to make people think about sharing and encourage the sector to work together. Sharing relevant information with the right person can mean that there can be earlier intervention and a better response to the situation.

It is often presumed that confidentiality comes first. People may think that this prevents them from sharing, despite existing legal rules that may override confidentiality, or processes that may result in the person agreeing to the information sharing. However, this does not mean that you shouldn't involve the person whose information you are sharing in the decision-making process. It is still best practice to seek consent.

B. Why is sharing not compulsory?

Family violence situations are highly variable. Sometimes, sharing information will be the best way to make sure agencies and practitioners are informed and people are kept safe. Sometimes, sharing may be inappropriate or unsafe.

The Act allows, but does not require, information to be shared so that agencies and practitioners can continue to use their professional judgement. You need to weigh up the pros and cons, and decide whether you should share personal information in the particular circumstances. **Use your professional judgement to make a decision**. Factors such as what it will take to keep people safe, and how to maintain trusted relationships, will be important. Talking to the person whose information you hold will often help you to make that decision.

PRINCIPLE FOUR

You can share information for specific purposes

The Act gives you **legal authority to share** personal information for specified purposes. You can share information proactively or in response to a request. The specific purposes that you may use, request or share information for are:

- to help ensure that a victim is protected from family violence
- to make, or contribute to, a family violence risk or needs assessment
- to make, contribute to, or carry out a decision or plan related to, arising from, or responding to family violence.

You can share information with another agency or practitioner if you reasonably believe that sharing the information will help the other person achieve one of the specified purposes. Making a decision about whether to share will require you to use your professional judgement based on the context you're working in, taking into account the victim's views on sharing the information.

You will also need to think about which pieces of information you hold is relevant to the specified purpose. For example, some information you hold might be relevant to undertaking a risk assessment, but may not be relevant for making a safety plan. You shouldn't share any more information than is necessary to achieve the specified purpose that you or the requester has identified.

The specified purposes cover the areas where those working in the sector most commonly need to share information, so the sector can work together to address family violence. The specified purposes also reflect the areas where there's most obvious benefit from sharing information or the most obvious need to share information to prevent or address violence. When deciding whether to share, you must keep in mind that helping to protect a victim from family violence overrides confidentiality and the Privacy Act.

You may make or receive a request verbally (by phone or in person) or in writing. Remember to record any requests you make or receive, including the relevant purpose and the steps you took to get in contact with the person whose personal information you want to share. See Principle 7 for more information about recording decisions.

If you want to share personal information for any other purpose, you need to make sure you have legal authority to do so. Remember you can always share information if you come across evidence of serious safety risks or criminal offending that are relevant to Police, Oranga Tamariki, or other authorities.

A. How do I request information?

If you are the person **requesting** information, you should make it clear which of the specified purposes applies to your situation, and what information you need. The clearer you are, the easier it will be for the other agency or person to agree to the request.

Don't ask for more information than you genuinely need or for information that is not relevant to your role. You should offer to discuss the request with the person if there are concerns.

You might want to provide feedback to the person who shared the information with you after you have used it. Feedback loops can be an important way to improve information sharing practice and create a better understanding of what types of information is useful to share. However, remember that you can only share personal information under the Act for one of the specified purposes. This means you often will not be able to tell the person who shared the information exactly what you did with it or what the outcome was. You can, however, let the person know if what they gave you was helpful and whether you used it for the purpose it was requested.

B. How do I respond to a request for information?

If you **receive a request** for personal information from another agency or practitioner, you can provide the information as long as you've got good reason to think that:

- the agency or practitioner is covered by the Act, and
- they need it for one of the specified purposes, and
- the information you hold is relevant to the purpose.

Make sure you are satisfied that you know the person making the request is covered by the Act. Without knowing who it is that is asking for the information, you won't be able to know why they need it and what they will do with it.

Often it will be clear that one of the specified purposes applies and that some of the information you hold is relevant for that purpose. For instance, you may have a working relationship with the other agency or practitioner and have a good understanding of what their role is and what they will do with this type of information.

If it's not clear whether the information fits one of the purposes or if it's going to be relevant, you should **talk to the other agency or practitioner** to find out more. You can ask the other person what information they need and why they need it. Verifying a request doesn't mean a lot of paperwork. If you're satisfied the other person's reasoning meets one of the specified purposes, you can share the information.

You can say no to a request if you don't think the information you have will be relevant to the person's role or the purpose they want to use it for. Likewise, if you do not think the person has justified their request, then say no. Give the person a link to this Guidance and suggest that they come back to you when they can clearly show what purpose they need it for.

Make sure you make a note of the request, including which specified purposes apply, your response, and record the information you send (if any). See Principle 7 for more information about recording decisions.

> Make sure you are satisfied that you know the person making the request is covered by the Act.

CASE EXAMPLE

Sharing information for a permitted purpose

Divya is a social worker who requests information from Andre, a primary school teacher. She asks for information about one of Andre's students, Stuart. Andre knows that he has a duty to consider sharing information as he is classified as a social services practitioner under the Family Violence Act 2018. However, he has not worked with Divya before and is unsure about some elements of her request.

Andre goes back to Divya and asks her for some more information. After talking with Divya, Andre is satisfied that she is a person covered by the Act and that she will use the information about Stuart for one of the permitted purposes.

As Stuart is a minor, Andre knows he should get consent from a parent. He knows that Stuart's father is a safe person to ask, so he approaches him for consent to share the relevant information with Divya. Stuart's father consents to Andre sharing.

Andre shares the relevant information with Divya. He then records what information he chose to share with Divya, why he shared it, and that Stuart's father consented to the sharing.

C. How do I make a proactive disclosure?

Information sharing does not have to be triggered by a request. You can share relevant information for a specified purpose **even if there is no request** for information. Proactive disclosures can help people get relevant information earlier, meaning family violence risks can be responded to more quickly.

If you think that another agency or practitioner could use the information you have for one of the specified purposes, then you can share the relevant information with them. While you may not be the practitioner making the plan, you might have information that could help. Whether you should proactively share will depend on the specific circumstances and should be based on your own professional judgement.

Think about who you could share with, what information is relevant for them, and what specified purpose they would use the information for. Talk to the victim and seek their consent to share proactively – engaging them in the process can help to restore their power and control.

If you don't think the recipient will be able to use the information for one of the specified purposes, you should not share it with them (unless there's another legal rule that applies). Remember that **the information is someone's story**, and you should think about the impact the sharing could have on that person when deciding whether to share.

D. When can I share information to protect a victim?

You can share information whenever you think it would help another agency or practitioner intervene to protect a victim from family violence. Always remember that people's safety comes first. **Don't wait to be asked** if someone is at risk if you know that another agency can step in to protect them.

Common examples where you might share to protect a person's safety include:

- reporting events to Police, as first responders
- raising reports of concern about child welfare to Oranga Tamariki
- providing a victim's phone number and address to an agency who can provide help
- making sure that emergency shelter or housing is available.

E. What is a risk or needs assessment?

You can share information to make, or contribute to, a family violence risk or needs assessment. A risk or needs assessment usually involves putting together a series of relevant factors, such as:

- details of previous and current incidents – some types of violence (e.g. strangulation) raise particular alarm bells
- whether the level of violence appears to be escalating or decreasing
- how likely the violence is to occur or recur, and how imminent the risk may be
- what harm the victim and others have suffered (e.g. injuries or distress) and the level of fear that they are expressing or displaying (if they are able to do so)
- what protective factors exist (e.g. family support for victim, perpetrator is in prison)
- what steps are necessary to make sure the victim is kept safe and/or the perpetrator is held accountable
- what other pressures may be contributing to the situation and need to be resolved (e.g. drug or alcohol dependency, mental health problems).

A risk or needs assessment may be **formal** – for example you might be involved in developing an assessment under a regular interagency arrangement, such as the Integrated Safety Response, Family Violence Interagency Response System, or Whāngaia Ngā Pā Harakeke.

A risk or needs assessment may also be informal – for instance you may have a telephone call with another agency where you decide you need to work together to assess and support a whānau or family.

The *Risk Assessment and Management Framework* has been developed specifically for agencies across the family violence sector. It provides a consistent way of talking about risk and you should use it as your main reference point. You can access it here: **www.justice.govt.nz/assets/Documents/Publications/family-violence-ramf.pdf**

F. What is "making, contributing to, or carrying out a plan"?

You can share information to make, contribute to, or carry out a decision or plan related to, arising from, or responding to family violence. Plans, or safety plans, can be used to manage the risks and effects of family violence. Planning and implementing plans may be formal (such as in regular interagency arrangements, or in mandated programmes) or informal (with agencies working together to support a whānau or family).

Forming and carrying out a plan may include steps such as:

- deciding what interventions would be most effective
- deciding which agencies are best suited to address the needs of a person, family or whānau (e.g. parenting support, counselling, or addiction services)
- referring the case to those agencies and identifying a lead agency if required
- reviewing progress to see whether people are responding well to a plan, and whether the risks are increasing or decreasing
- identifying whether new factors have arisen that affect the original plan, and modifying the plan accordingly
- reporting back on the original plan if the agency isn't able to assist and the needs may remain unmet (e.g. if a Report of Concern doesn't meet Oranga Tamariki's statutory threshold for intervention, then it's important for Oranga Tamariki to report back so that different steps can be taken to protect the children)
- deciding when a plan has run its course and the people no longer need support.

Information sharing for this purpose doesn't just cover the initial process of forming a plan. It covers "carrying out" the plan too. This recognises that the process of making, contributing to and carrying out plans is dynamic – it is often an **ongoing process** rather than a single intervention. A plan can change as people's situations change.

G. How is this different from what I could share before under the Privacy Act?

The Family Violence Act urges you to consider sharing information in the first instance. In contrast, the Privacy Act has a starting point of not sharing, unless a specified ground applies.

While the Privacy Act allows people to share information with agencies that can intervene to protect people from serious safety risks, this has been interpreted as a high threshold. The Privacy Act is written in general terms because it applies to every situation, not just in family violence situations. It doesn't always cater for the complexities in the family violence sector and doesn't recognise that small, sometimes trivial information can paint a bigger picture of risk or indicate a pattern amounting to cumulative harm.

For further information about privacy and the Privacy Act, see **www.privacy.org.nz/**.

> The Family Violence Act urges you to consider sharing information in the first instance.

PRINCIPLE FIVE

You must only share relevant information

You must only share information where you believe that the information will be relevant to help achieve one of the specified purposes. What information is relevant will depend on the context of each situation. Your professional experience is likely to give you strong instincts about what's genuinely useful to share.

A. What information is relevant?

It's impossible to set out exactly what relevant information looks like. What is relevant to one person for one purpose may not be relevant to another, as they may use the information for different reasons depending on their role. When thinking about whether a certain piece of information you hold is relevant, you should consider:

- **Who** is making the request?
- **Why** are they making the request?
- **What** kind of information are they requesting?
- **Which** specified purpose do they need the information for?

If you are unsure that the information is relevant to achieve the particular specified purpose, check with the person making the request. You can use the questions above to guide you in your conversations with the requester. Remember that the information you are dealing with is a person's story and you are merely a custodian of that information. Sharing irrelevant information can create unnecessary risk or harm, and may amount to bad faith. The person whose information it is should be kept at the front of your mind at all times during the information sharing process.

Relevant information may look like:

- details of what happened during current or past family violence episodes (e.g. Police reports, or statements from participants or witnesses)
- effects of family violence on the victims and their whānau (e.g. physical harm, or visible or stated distress)
- factors that may contribute to the violence or its severity (e.g. mental health conditions, alcohol or drug addiction, current financial pressures, family history of violence, or housing or education difficulties)
- criminal history relating to family violence
- a pattern of behaviour – separate incidents that may seem trivial in isolation, but that add up to family violence
- past history of services that relate to family violence, and outcomes of engagement.

You're likely to be able to quickly identify information that's clearly relevant for a specified purpose. Share that information first, and then think whether there's further information that might also be relevant. Sometimes, you might not even need to identify someone to share the information.

> You must only share information where you believe that the information will be relevant to help achieve one of the specified purposes.

B. What information isn't relevant?

It's important to only share the details that are necessary to achieve the specified purposes that you, or the person you are sharing with, have in mind. Only share personal information when you need to and share no more than necessary. Value statements about the victim or associated persons, gossip, rumour, or information that is designed to be disrespectful will not be relevant and should not be shared. These types of statements or information can be harmful and may put a person at greater risk. Remember to put yourself in the shoes of the person you're sharing information about - think about what information people would need to know to keep you safe, and what would be unnecessary or irrelevant detail.

CASE EXAMPLE

Discretion in sharing and relevant information

Piripi, a Whānau Ora worker, requests information from Anne, a general practitioner, about the Smith whānau. He is concerned because a client of his, Henri Smith (aged 4), has not kept his hospital appointment on three occasions and has been discharged from the waiting list.

Anne knows that she has a duty to consider sharing information. She decides that it is appropriate to share information in this case, knowing that Piripi wants to use the information to assess Henri's risk.

However, Anne has a large file of information about the Smith whānau and knows that not all this information relates to the request about Henri. She also knows that some of this information is gossip and unsubstantiated information.

Anne approaches the whānau and asks for consent to share the relevant information with Piripi, but they don't respond to her texts or phone calls. Anne, using her professional judgement, decides to only share Henri's history of injuries that are consistent with family violence and notes regarding a recent influenza infection. Anne then records what information she chose to share with Piripi and why. She also records that she was unable to obtain consent from the Smith whānau, and the efforts she made to contact them.

When she manages to get in touch with the Smith whānau, she lets them know that she shared Henri's information with Piripi.

PRINCIPLE SIX

You should check the information is accurate

Before sharing information, you should take reasonable steps to check the information is accurate, up to date, and complete. What steps are reasonable will depend on the particular circumstances. This is a requirement under the Privacy Act and continues to apply under the new information sharing laws – you can find out more here: **www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/accuracy-etc-of-personal-information-to-be-checked-before-use-principle-8/**

One of the simplest ways to check information is up-to-date and accurate is to talk to the person whose information it is. This can help ensure you don't share unsubstantiated information or gossip, and reflects good practice. Sometimes you may not be the person who collected the information. However, you still need to take steps to ensure any information you share is correct before you share it. If you are sharing information and you are not sure that the information is accurate, up to date and complete, then make that clear when you share the information. This is one way you can reduce the risk of causing harm or putting someone in danger.

If you have shared information that you later find out is inaccurate, contact any agency that you believe may be using that information and tell them what the correct information is.

There might be situations where you don't know if information is accurate, but you still choose to share. For example, if you have suspicions that family violence is occurring but no definite evidence. Your professional experience is likely to give you strong instincts about what to share in these situations, and you should take care not to portray these suspicions as fact.

***For example,** it is fine to talk to Oranga Tamariki to report potential risks to a child, even if you're not sure whether all the information you're giving is correct. It's Oranga Tamariki's job to decide whether to investigate: its staff have the skills and the statutory powers to find out what's actually happening and whether there's a problem.*

Similarly, if you believe that a crime has been committed, you can talk to the Police. It's up to the Police to decide whether to make further enquiries.

The Privacy Act allows people to correct information about themselves. If someone contacts you wanting to correct the information you hold about them, follow the procedures set out on the Office of the Privacy Commissioner's website at: **www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/correction-of-personal-information-principle-seven/.**

A. How accurate is "accurate"?

Factors to consider when determining whether information is sufficiently accurate, up to date, or complete include:

- what purpose the information will be used for
- whether the recipient will or may believe that it is factual
- whether the recipient will rely on it to make a decision about an individual, including a decision about whether to provide or withdraw services, what services would be appropriate, or how to provide those services, and
- whether the information is negative, or may be seen as negative, about an individual.

> ***For example,*** *it is better to share objective concerns and statements of fact rather than assumptions or subjective impressions of a situation. It's important to record and share information as factually and impartially as possible.*

Most obviously, make sure that you are **sharing information about the right person**. It's easy to get records confused, particularly where people have common names, names that can be spelt in different ways, or names that get translated into English in different ways. Double-check against additional information like gender, date of birth, place of residence and distinguishing features (e.g. photos, if available) to make sure you've got it right.

Other reasonable steps to check the accuracy of the information may include:

- discussing the information with the individual
- cross-checking the information with another agency or individual in the sector, or
- considering other information on record about the person to see whether there are unexplained discrepancies.

B. Do I have to guarantee that information is accurate before I share it?

Occasionally, despite your best efforts, information may still be inaccurate. You're not required to guarantee that information is right before you pass it on. However, you do need to take reasonable care.

You have much stronger obligations to make sure that the information is accurate if you're sharing information that you are claiming is factual (or that people will think is correct because you're the source of it), or information that other people need to rely on. Also, if the information could create trouble for someone, it's particularly important to make sure it's as correct as possible.

> Occasionally, despite your best efforts, information may still be inaccurate.

PRINCIPLE SEVEN

07

You should record reasons for your decisions

If you receive a request from an agency or practitioner to share personal information that is relevant for one of the specified purposes, make sure you **keep a record** of the request, including:

- who made the request
- the details of the request itself
- whether or not you agree to the request
- your reasons for sharing or deciding not to share
- how you attempted to get consent and whether consent was obtained, and
- if you agree to the request, note what information was sent and when you sent it.

If you make a request for personal information to another agency, keep a record of the request (including what you wanted and why you wanted it) and note who you spoke to. Make sure your notes are neutral and factual, and avoid recording personal judgements.

If you decide to disclose information proactively to another agency, note why you believe that releasing the information would achieve one of the specified purposes, whether you had consent to share, what information was sent and when it was sent.

A. Why is keeping notes important?

Record keeping is important for several reasons. It will help you **explain** what you've done and why, to the person whose information you've shared. It can help you explain your decision to the Privacy Commissioner or your professional organisation, and can be used to demonstrate that you were not acting in bad faith when sharing information. It will also help your agency look back at what information has been shared in the past and make more consistent decisions about sharing information in the future.

Keeping records of your decisions doesn't need to be resource-intensive. Brief notes will do. Include the dates **when** things happened, **what** was decided, and **who** was involved. Note **why** you chose to release or withhold information. It's still important to keep notes **even when you decide not to share**.

If you have level 2 Ministry of Social Development accreditation, you should use the system you have in place to deal with privacy requests. For more information, see: www.msd.govt.nz/what-we-can-do/providers/social-services-accreditation/accreditation-standards.html.

If you're sending an email or a letter, put it in the client file. If you've shared information by telephone call and you can't type straight into the client file, make handwritten notes of what was said and add them to the client file later.

CASE EXAMPLE

Keeping notes explaining your decisions

Alice, a Tamariki Ora Registered Nurse, is concerned about Janet and her new born baby, Charlotte, after her first home visit for Charlotte's well child check. Alice wants to share information about Janet and Charlotte with her manager, her co-workers, a family violence social worker and a non-regulated kaiawhina who support parents of young children in the same integrated Māori health and social service organisation that Alice works for (a government funded family violence service provider).

Alice asks Janet and her grandmother, Katherine (the family spokesperson), for consent to share information with her manager, her co-workers, the social worker and non-regulated kaiawhina about the current situation. This includes disclosure of historical family violence, gang affiliation and post-traumatic stress disorder. Janet and Katherine give their consent.

Alice shares information about Janet and Charlotte's family situation with her colleagues. She knows that she can share with her manager, her co-workers and the social worker under the Family Violence Act. She also knows that, as she has Janet and Katherine's informed consent, she can share with the non-regulated kaiawhina, even though she is not a person covered by the Act.

Alice records what information she chose to share and why, who she shared it with, and that the information was shared with Janet and Katherine's consent. Alice lets Janet and Katherine know of the sharing afterward.

PRINCIPLE EIGHT

You have legal protection from liability when you share information, unless you share in bad faith

If you share information in accordance with the rules under the Act, and follow this Guidance, then you will be **immune from liability**, unless you were acting in bad faith. This doesn't stop someone from making a complaint, but it does provide you with legal protection if a complaint is made. This protection means you can be confident when sharing information that you genuinely think is necessary to share to help people involved in a family violence situation.

The only exception to protection from liability is where you have shared the information in bad faith. Bad faith can arise where someone has malicious or hidden motives, hasn't attempted to comply with their legal obligations, or acts carelessly or recklessly. For example, bad faith may arise where you don't check who someone is before sending them information, or you send a full document rather than taking the time to assess whether the information is relevant.

The Act doesn't force you to share information – whether or not you share is a judgement call for you to make. You need to be aware of other rules that may apply. In particular, consider the following:

- Has an agency given you a statutory demand for the information? If so, you will need to comply with that demand.
- Is there a warrant or other form of court order that requires you to supply the information? If so, you need to provide the relevant information.
- Are you a mandated programme provider who has concerns for the safety of the victim, the perpetrator, or others? If so, you need to report those concerns to the court Registrar and the Police and – if a child is involved – to Oranga Tamariki.

A. What happens if there is a statutory or court-ordered demand for information?

Some government agencies can issue statutory demands for information (not solely in relation to family violence). Similarly, agencies will have to produce information if it is covered by a warrant, or other lawful demand for the information. It should be plain from the demand what is required.

For example, Oranga Tamariki or Police can make a statutory demand under section 66 of the Oranga Tamariki Act for information for the purposes of determining whether a child or young person is in need of care and protection.

Statutory requests should clearly state which legal provision applies, and should specify what information is required. If the request is not clear, then question it.

> The only exception to protection from liability is where you have shared the information in bad faith.

B. What information can I not share?

Sometimes, other statutes will prohibit information sharing. You need to know if there are any rules that apply to you.

For example, under the Family Dispute Resolution Act 2013, information that emerges in dispute resolution talks is privileged and can't be shared without consent.

(a) Information held by the court

Information that is under the control of the courts is governed by court rules. It isn't Ministry of Justice information – the Ministry's role is to support the administration of the courts by managing court resources and holding information on behalf of the courts. This Guidance and the information sharing provisions in the Act **do not apply to court information or court staff**.

There can also be statutory rules that apply. For instance, reports produced by welfare or child protection agencies for the Family Court may not be disclosed – even to the parties to the court case – without the court's permission.

(b) Privileged information

Information is privileged when there are legal grounds to withhold it under the Evidence Act 2006, in order to preserve confidentiality and protect certain relationships. The Evidence Act specifies what kinds of information are protected by privilege, including legal privilege, religious privilege, medical privilege and journalistic privilege.

Similarly, the right against self-incrimination remains in place. This allows a person to refuse to provide information that would be likely to make them appear guilty under New Zealand law.

C. Why can't I use information for personal reasons?

If you are authorised to access an agency's systems for your work purposes, you must only use personal information for those purposes. You must not search for, read, copy, disclose or use information from those systems for your own personal reasons.

Recognise that **you are a kaitiaki, a custodian, of the information** that you have access to as part of your work. Behind every piece of personal information there's at least one person, who deserves respect and dignity. Treat that information accordingly.

Breaching this rule will likely amount to acting in bad faith. Using information on work-related systems for your own personal motives is a serious breach of trust, privacy and ethical responsibilities. You will not be protected from liability under your professional codes of ethics, the Privacy Act, or other legal rules.

For example, *suppose you find out through your work that someone you know is involved in a family violence situation. You must not take that information and tell other family members or friends about it, even if you think that they may be able to help to resolve the situation, or you think that the information might be useful to them in court proceedings (such as child custody discussions). You have to keep your official role and your personal role separate.*

Similarly, you must not look up family members or friends on an agency database for your own personal reasons, such as checking out whether your daughter's new boyfriend has a history of family violence.

PART III

Collecting, storing and keeping information

The Privacy Act sets out 12 principles that describe how personal information should be collected, used, stored and disclosed. Most of these principles continue to apply to the information you collect, share and use under the Family Violence Act. Don't forget that the things you record on a file should be objective and based on fact. That way, when you share that information, you won't be at risk of sharing anything irrelevant or incorrect.

Under the Privacy Act, a person can complain to the Office of the Privacy Commissioner if they have concerns that their privacy has been breached.

For further information about privacy and the Privacy Act, see **www.privacy.org.nz/**.

A. How should personal information be collected?

Wherever possible, you should collect personal information directly from the person concerned. Being transparent about why you are collecting information, and what you will use it for, builds trust and makes people more confident that their information will be secure and treated properly.

For further information on collecting information, see **www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/manner-of-collection-of-personal-information-principle-four/**.

B. How do I keep information safe?

Agencies that share personal information must take reasonable steps to make sure that the information is transferred safely, so that it does not end up in the wrong hands. The information must also be stored safely once it is received. The more sensitive the information is (that is, the more distress or harm it could cause if it is stolen or goes astray), the more care you have to take. Information about family violence is usually highly sensitive.

If you discover that personal information has been, or may have been, lost, misaddressed or misused, or may otherwise have ended up in unauthorised hands, you must take any reasonable steps that you can to retrieve the information and ensure that it is not further disclosed. You should then assess how the incident occurred, and take whatever steps are reasonable to prevent such an incident from happening in the future.

For comprehensive advice on keeping information safe when sharing and managing data breaches, see **www.privacy.org.nz/data-breaches/data-safety-toolkit/**.

For easy practical tips on computer security, check out NetSafe's website (**www.netsafe.org.nz**) or the "Get Cyber Smart" information available on the CERT website (**www.cert.govt.nz**).

C. How long should I keep information for?

Information can lose its value over time. People's circumstances change, and information that you hold is likely to become out of date. The Privacy Act requires you to think about whether you can still use the information for the reason you got it. If the answer is no, and if there's no other legal rule saying you have to keep it, then you need to delete it.

There's no single answer to how long an agency should keep information. It depends on the context. When working out how long you need to keep information, remember that if you keep it, you're responsible for keeping it safe.

For advice on keeping information, see: **www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/agency-not-to-keep-personal-information-for-longer-than-necessary-principle-nine/**.

D. Do people have a right to access their information?

People have a right to seek confirmation that an agency holds their personal information, to ask agencies for access to that personal information, and to correct any information held about them. Requiring agencies to be open about what information they hold empowers the person concerned, supports open and collaborative relationships, and encourages agencies to act responsibly.

Public sector agencies, such as government departments, aren't allowed to charge people for access to their information (except in limited circumstances with the Privacy Commissioner's permission). Private sector agencies, such as NGOs, are technically allowed to charge a reasonable fee for making information available – for example to cover photocopying and courier costs. If it's only a small amount of information, think about whether it is worth the hassle, particularly if you are dealing with someone who needs the information but doesn't have any money.

For more information on providing access to personal information, see: **www.privacy.org.nz/the-privacy-act-and-codes/privacy-principles/access/**.

> People have a right to seek confirmation that an agency holds their personal information.

APPENDIX 1

Terms used in this document

"Family violence" means violence inflicted against a person (the victim) by someone (the perpetrator) with whom that person is, or has been, in a family relationship. Violence can be physical abuse, sexual abuse, or psychological abuse. It includes single acts and patterns of behaviour that may be coercive or controlling, or that does or may cause cumulative harm. See section 9 of the Family Violence Act 2018 for the full definition.

"Victim" means a person who has, is, or may be experiencing family violence, or affected by family violence (either now or in the past). A victim can be of any age or gender and, particularly in cases involving children, can include those who are not the specific target of abuse but may experience it nonetheless.

"Perpetrator" means a person who has (or may have) inflicted family violence, or a person who is (or may be) inflicting family violence. It does not matter that the perpetrator may not be charged, prosecuted or convicted of or for an offence.

"Family relationship" includes relationships between spouses, partners, family members, people who live in the same household, or people who have a close personal relationship (based on the nature, intensity and duration of the relationship). They are not limited to romantic or intimate partnerships, and include a wide range of relationships, such as whānau relationships, relationships between grandparents and grandchildren, or relationships between siblings.

"Information sharing" includes requesting, receiving, or disclosing personal information to or from another agency or individual, exchanging personal information between separate parts of the same agency, and using personal information.

"The sector" includes specified family violence agencies and social services practitioners – see pg 5 of this Guidance.

"Specified purpose" means one of the three purposes for which personal information can be shared. See Principle 4 of this Guidance.

"Personal information" has the same meaning as in the Privacy Act 1993: it is information about an identifiable, living human being. For example, personal information may include medical information (such as information about injuries, sexual information, mental health or addiction information), criminal history, family circumstances, involvement with social services, and financial details.

"Psychological abuse" includes threats of physical or sexual abuse, intimidation or harassment, damage to property, ill-treatment of pets and animals, and financial or economic abuse. It includes putting a child at real risk of seeing or hearing abuse of a person who the child has a family relationship with. It also includes hindering access to aids, devices, medication or other support that likely affects a person's quality of life.

"Bad faith", for the purposes of this document, includes situations where someone shares information with malicious or hidden motives, hasn't attempted to comply with their legal obligations, or acts carelessly or recklessly when sharing information. There may be other situations that also constitute bad faith. For more information see Principle 8 of this Guidance.

"NGO", for the purposes of this document, means a non-government organisation that is wholly or partly funded by government to provide family violence services.

APPENDIX 2

Who is not covered by the legislation?

Any agency or person who isn't listed in the Act is not covered and cannot share under the Act. These agencies and individuals may still be able to share personal information, but only if other laws allow it. For example, the Privacy Act enables everyone to share personal information to prevent or lessen a serious threat to someone's health or life.

The Family Violence Act does not cover information sharing that involves:

- **Non-listed government departments or public sector agencies**. Only the specified government agencies are covered. All other public sector agencies will be governed by their own legislation, by their own codes of practice, or by the Privacy Act.
- **NGOs that provide family violence services without receiving any government funding**. These agencies will need to use the Privacy Act provisions, or other relevant legislation (for example, the Oranga Tamariki Act), for any information sharing that they undertake.
- **Members of the public**, such as family or whānau of victims or perpetrators. They can report information to authorities in the usual way. The public can also receive information from agencies when it is permitted under the Privacy Act (for example, for safety reasons or with the consent of the person). Family and whānau are often an integral part of preventing future violence or supporting victims of violence.
- **Court information and court staff**. Information that is under court control is subject to specific rules that allow it to be disclosed on a case-by-case basis. You need to approach the court directly to access this information.

New Zealand Government