Sharing information safely

Guidance on sharing personal information under the Family and Whānau Violence Legislation Bill

Ministry of Justice

DRAFT for consultation

MINISTRY OF JUSTICE
Tāhū o te Ture

New Zealand Government

[Publication details]

Foreword

Table of Contents

WHAT THIS GUIDANCE COVERS

A 'how-to-guide' to help the family violence sector apply information sharing rules and manage information safely

RULES THAT APPLY

Legislation

- Domestic Violence Act 1995 (that will be amended by the Family and Whānau Violence Legislation Bill)
- Privacy Act 1993
- Oranga Tamariki Act 1989
- District Court Act 2016
- Senior Courts Act 2016

Codes of Ethics

You won't breach a code unless you act in bad faith

Other rules

In some circumstances, special rules will apply (eg, warrants)

MANAGING INFORMATION

COLLECT

- Collect information when it is necessary for the job
- Collect directly from the person unless an exception applies

STORE

- Keep information safe and secure
- Keep only as long as necessary
- Manage privacy breaches appropriately

SHARE

- Share information for permitted purposes
- Share only relevant information
- You have duty to consider sharing

PROVIDE ACCESS

- When people ask for information about themselves, you must provide access unless there is good reason not to

TO WORK TOGETHER TO ADDRESS FAMILY VIOLENCE

- Provide timely and effective responses
- Better mitigate risk

Part I: General information

A. What is this document for?

The Domestic Violence Act 1995 ("the Act") will be amended by the Family and Whānau Violence Legislation Bill. Once amended, the Act will include rules about when personal information can be shared, which work alongside rules in other legislation, such as the Oranga Tamariki Act 1989 and the Privacy Act 1993. This guidance is intended to assist those in the wider family violence sector to meet their legal obligations and work together to address family violence.

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

- protect people from family violence, improve their lives and make it easier for them to get the help they need
- encourage the family violence sector to share personal information and work collaboratively
- ensure information sharing occurs in a way that is safe and appropriate
- provide the family violence sector with confidence that the law will protect them when they share information appropriately.

This guidance provides practical help for people who need to apply the information sharing rules in their everyday work. It includes some basic diagrams, explanations and case examples to help illustrate what to do.

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

B. What does the guidance cover?

The guidance discusses how personal information is to be treated in the family violence sector. It covers the information sharing provisions in the Act and how these relate to rules in other legislation, such as the Oranga Tamariki Act 1989 and Privacy Act 1993.

While the document focuses on the rules around information sharing, it also includes guidance on the other key parts of the 'life-cycle' of personal information from collection through to destruction.

The document is split into five parts:

- Part I: General information
- Part II: Sharing information – making sure the right information is shared at the right time with the right people
- Part III: Storing information – keeping information safe to prevent privacy breaches
- Part IV: Providing access to information – ensuring that people have access to their information and can correct it
- Part V: Collecting information – knowing the dos and don'ts when collecting information from people.

C. How "personal" does "personal information" have to be?

Personal information is any information about an identifiable, living human being. It doesn't have to include someone's name, it doesn't have to be secret, and it doesn't have to be sensitive. It just has to be about someone who is identifiable in the circumstances.

For example, a person might be identifiable because you can tell who they are from the description of their circumstances, where they live, or who they are associated with.

In the context of family violence, 'personal information' is likely to include information about a victim, perpetrator, child, family or whānau members, or support people.

Personal information will range from basic information like names and contact details, through to highly detailed information about people's lives. Examples could include detailed medical information (such as sexual information, mental health or addiction information), criminal history, family circumstances, involvement with social services, and financial details.

The sensitivity of personal information will vary – that is, the harm that it might do in the wrong hands will differ, depending on the circumstances. For example, 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, their contact details may be among the most sensitive information that they provide.

D. Who can share under the Family Violence legislation?

New section 124U of the Act defines the family violence agencies and individuals that can share personal information under new part 6B of the Act.

Those agencies and individuals consist of four broad categories:

(a) Specified government agencies
(b) Government-funded (wholly or partly) non-governmental organisations (NGOs) that deliver family violence services
(c) School boards and early childhood services
(d) Social services practitioners.

To keep it simple, this document refers to all these agencies and individuals as "**the sector**".

The "specified government agencies" are the Accident Compensation Corporation, Department of Corrections, Ministries of Education, Health, Justice and Social Development, Oranga Tamariki, New Zealand Police, Immigration New Zealand, District Health Boards, Housing New Zealand Corporation, and registered community housing providers.

Any new government or other agency that takes over the family violence functions of any of these existing government agencies will automatically be classed as a specified government agency.

These government agencies will, in some cases, be able to share information under other legislation. On rare occasions, other legislation may prevent the government agency from sharing personal information or restrict when information can be shared. The relevant government agency will be best placed to advise you when these situations arise.

Other agencies in "the sector" are school boards, licenced early childhood services, and NGOs that are partly or wholly funded by government to protect or help victims of family violence, or to work with perpetrators to stop them inflicting family violence.

"School boards" are any board (defined in section 60 of the Education Act 1989), a sponsor of a partnership school kura hourua, or the manager of a private school registered under section 35A of the Education Act 1989.

A "licenced early childhood service" includes any early childhood education and care centre, home-based education and care service, or hospital-based education and care service licenced under regulations provided for in section 317 of the Education Act 1989.

"Social services practitioners" are registered teachers (under the Education Act 1989), registered health professionals (under the Health Practitioners' Competence Assurance Act 2003) and registered social workers (under the Social Workers Registration Act 2003).

E. Why isn't everyone covered by the information sharing provisions?

The list of agencies and individuals that are permitted to share personal information under the Act is limited because information about family violence isn't everybody's business. The Act only covers agencies and individuals who specialise in addressing family violence, who are most likely to hold information that's relevant to family violence, or who are most likely to come across evidence of family violence in their work.

These are also the agencies and individuals that are best placed to make a professional call about whether sharing is desirable, whether it would be effective or create further risks, and who else might need to know the information.

At the community level, many of those working in the sector will know one another well and may be working closely together already. The Act and this guidance should enhance their ability to do so and help to make sure they handle that information in a safe and trusted way.

F. Who is not covered by the legislation?

Any agency or person who isn't listed in the Act is not covered. They may still be able to share personal information, but any information sharing will need to be permitted by other

law. 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 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, 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 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. They 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 people who are victims of violence.
- **Court information**. 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.

G. What legal protection do I have if I follow the law?

If you comply with the information sharing rules, as detailed in this guidance, you will be immune from legal liability and from any professional disciplinary processes, provided that you have not acted in bad faith.

This doesn't stop someone from making a complaint about you (for instance to the Privacy Commissioner) but it does mean that the complaint won't be upheld unless you have shared information in bad faith. Information sharing may be deemed to be in bad faith if it is:

- irrelevant information that is shared. You should identify the permitted purpose for sharing the information, and must share only the information relevant to that purpose (ie, you should not overshare information).
- shared with inappropriate people. Information should only be shared with those agencies and individuals listed in the Act that can take the appropriate steps in relation to the purpose for which it was shared.
- shared without a reasonable belief that the information being provided to another agency will assist them with a permitted purpose.

Bad faith doesn't necessarily require malice, it can be as simple as dishonesty.

The information sharing provisions in the Act work alongside other pieces of legislation that enable, require or prohibit information sharing. Provisions in other legislation will continue to operate as normal, the exception to this being the Privacy Act. The provisions in the Act take priority over the Privacy Act. This guidance provides some detail about when other legislation applies and when you should think about other obligations you have.

Terms used in this document

"**The sector"** includes any specified government agency listed in new section 124U of the Act. It also includes wholly and partly publicly funded NGOs that provide family violence services, school boards, licenced early childhood services, and registered teachers, GPs and social workers.

"Family violence" has the same meaning as that set out in new section 3 of the Act. It means **violence** inflicted against a person by someone with whom that person is, or has been, in a **family relationship**.

"Family relationship" means the relationships set out in the amended section 4(1) of the Act. This includes relationships between spouses, partners, family members or between people who have a close personal relationship (based on nature, intensity and duration of the relationship). It also includes the relationship between people sharing a household.

"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.

"**Permitted purpose**" means one of the three purposes for which personal information can be shared under new section 124V of the Act. These purposes are to help protect a victim from family violence, and for family violence risk or need assessments, or to make or carry out a decision or plan related to family violence.

"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 with, or prosecuted for, an offence.

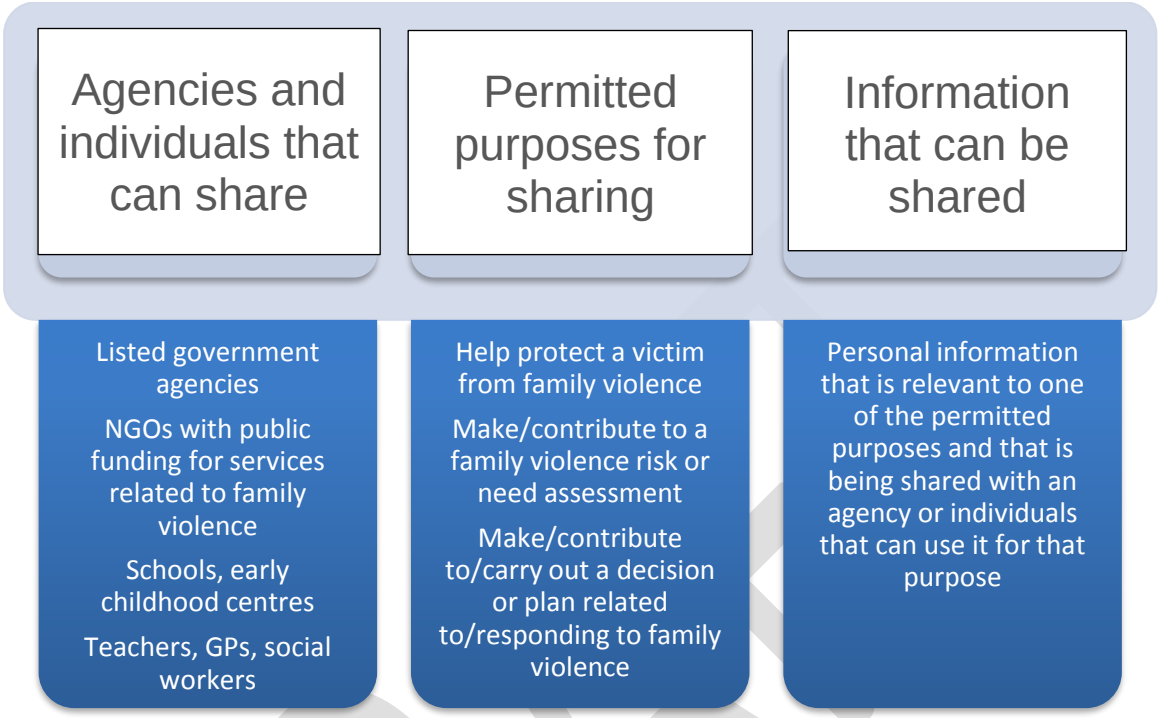
"Personal information" has the same meaning as in the Privacy Act: it is information about an identifiable, living human being.

"Psychological abuse" has the meaning set out in new section 3 of the Act. It 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 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.

"**Victim"** means a person who has, is, or may be experiencing family violence, or affected by family violence (either now or in the past).

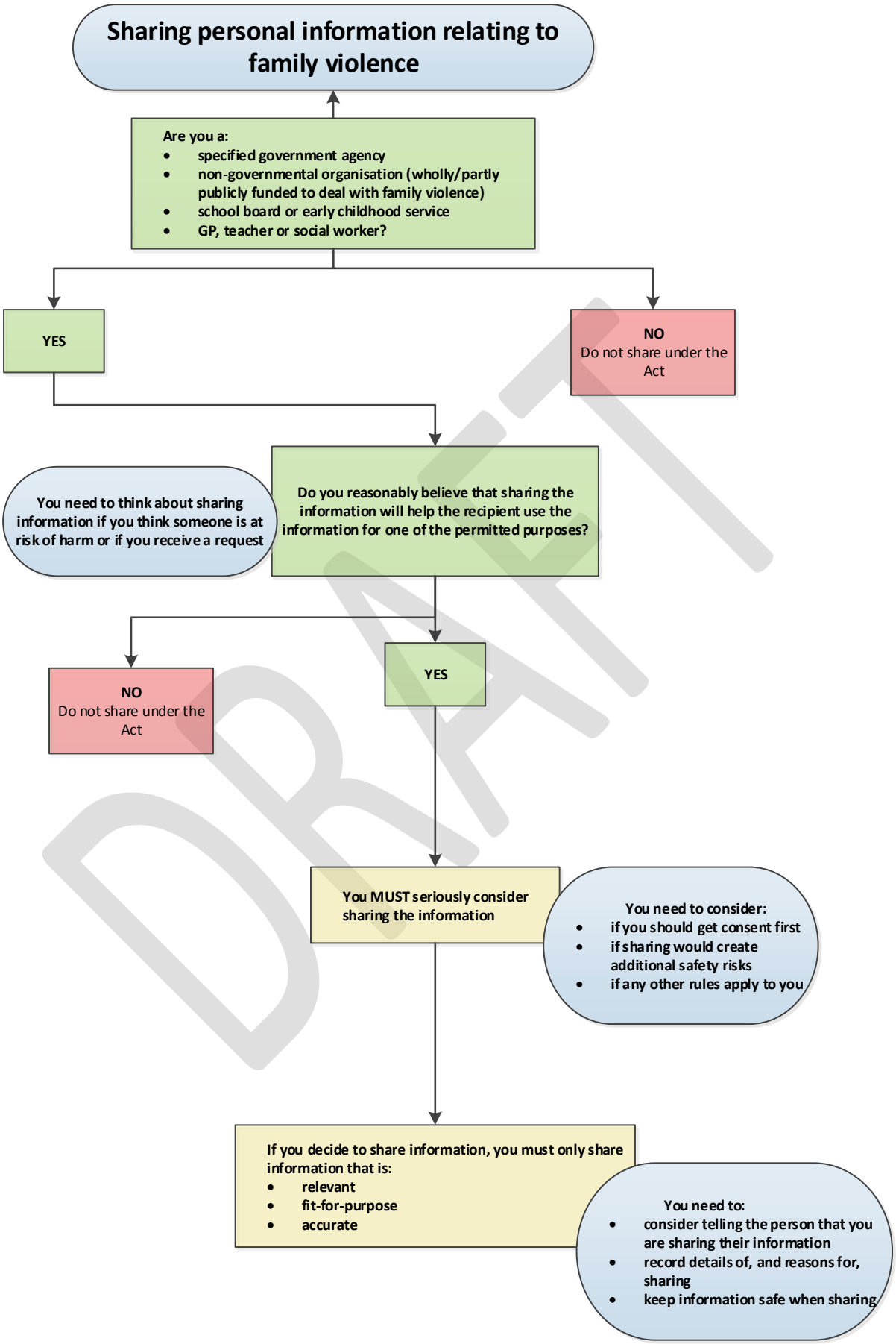
"**Violence**" has the same definition as in new sections 3(2) - (4) of the Act. It includes physical abuse, sexual abuse, psychological abuse, behaviour that is coercive or controlling, behaviour that causes or may cause harm. It includes not only single acts but also patterns of behaviour that have a cumulative effect amounting to family violence.

Part II: Sharing information



Summary of guidance on sharing information

1. Information can be shared for certain purposes
2. You have a duty to consider sharing
3. People's safety comes first
4. Only share relevant information
5. You must not use information for personal reasons
6. Consider getting consent, unless unsafe or impractical
7. Check that information is fit for purpose
8. Record reasons for decisions
9. Protection from liability for sharing


Sharing personal information relating to family violence
Are you a:
specified government agency
non-governmental organisation (wholly/partly publicly funded to deal with family violence)
school board or early childhood service
GP, teacher or social worker?
YES
NO
Do not share under the Act
You need to think about sharing information if you think someone is at risk of harm or if you receive a request
Do you reasonably believe that sharing the information will help the recipient use the information for one of the permitted purposes?
NO
Do not share under the Act
YES
You MUST seriously consider sharing the information
You need to consider:
if you should get consent first
if sharing would create additional safety risks
if any other rules apply to you
If you decide to share information, you must only share information that is:
relevant
fit-for-purpose
accurate
You need to:
consider telling the person that you are sharing their information
record details of, and reasons for, sharing
keep information safe when sharing

Information can be shared for certain purposes

The Act gives the sector legal authority to share personal information for the purposes listed in new section 124V(1) ("permitted purposes").

These permitted purposes are:

(a) to make, or contribute, to a family violence risk or need assessment
(b) to make, contribute to, or carry out a decision or plan in relation to family violence
(c) to help ensure that a victim is protected from family violence.

If you want to share personal information for any other purpose, you need to make sure you have alternative legal authority to do so. For example, the Privacy Act enables everyone to share personal information to prevent or lessen a serious threat to someone's health or life.

A. What is a risk or needs assessment?

A risk or needs assessment usually involves putting together a series of relevant factors, including:

- details of previous and current incidents – some types of violence (eg, 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 (eg, 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 (eg, 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 (eg, drug or alcohol dependency, mental health problems).

The Risk Assessment and Management Framework has been developed specifically for agencies across the family violence sector. It creates a consistent way of talking about risk and you should use it as your main reference point.

A risk or needs assessment may be **formal** – for example you might be involved in developing an assessment under a regular inter-agency arrangement, such as the Integrated Safety Response (ISR), Family Violence Inter-agency Response System (FVIARS) or Whāngaia Ngā Pā Harakeke (Whāngaia).

It 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.

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

Forming and carrying out a plan can 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 (for instance 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 (for instance 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 support 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. It can change as people's situations change.

Planning and implementing plans may be formal (such as in regular inter-agency arrangements, or in mandated programmes) or it may be informal (with agencies working together on the ground to help their respective clients).

C. When can I share information to protect someone?

You can share information whenever it would help another agency intervene to protect a victim from family violence. Give the information to the agency that can act on it effectively.

Remember that 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. Pick up the phone.

Common examples 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.

D. Communication is key

If it's not clear whether the information fits one of the purposes, or that it's going to be relevant, then talk to the other agency or agencies. Find out what they need and what they

would do with it. The better you understand their role, the more certain you can be whether sharing the information would fit one of the purposes for sharing and be genuinely useful.

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

- the agency is covered by the Act
- the agency needs it for one of the permitted purposes, and
- the information is relevant.

If there is **no request** for information, but you believe it would be beneficial to disclose information for one of the permitted purposes, think carefully about who needs it.

If a person will not be able to use the information for one of the permitted purposes, then don't send it to them (unless there's another legal rule that applies).

Conversely, if you think there's a good chance that the person will be able to use it for one of the permitted purposes, then you are allowed to send it.

E. How do I verify that a request for information is for a permitted purpose?

Often it will be obvious that one of the permitted purposes applies. For instance, you might be working jointly with a family and the request is part of an ongoing conversation. Or you may have a regular working relationship with the other agency and have a strong understanding about what their role is and what they do with information of this type.

But there can be grey areas. You need to make sure you have enough information to be able to make that judgment call.

If an agency is asking you for information, it needs to give you enough detail about why it needs that information so you can be reasonably certain that one of the permitted purposes applies.

If you're not sure why the person wants it (even if you work together routinely), then ask.

This doesn't mean a lot of paperwork or bureaucracy. If you get a request out of the blue and you are unclear why the person is asking for the information, a phone call to the right person is probably all that's needed to understand the situation and understand what is needed.

If, in your professional judgment, you still think the person hasn't justified a request, then say no. Give the person a link to this guidance document and suggest that they come back to you when they can clearly show the permitted purpose.

If you think they're asking for more information than they need, then provide the information that you know you are allowed to provide and say no to the rest.

Make a note of the request and your response, and keep a note of the information you send.

F. Make it clear why you need information if you are requesting it

If you are the person requesting information, you'll need to make it as clear as possible which of the permitted 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 than you genuinely need. Offer to discuss things if there are concerns.

G. Proactive disclosures

Information sharing is not always triggered by a request. Don't be afraid to engage proactively with other people in the sector where sharing information will enable you to fulfil one of the permitted purposes. Sharing may also be part and parcel of what you have to do.

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

The Privacy Act allows you to share information for similar reasons to the Act. For example, the Privacy Act allows people to share information with agencies that can intervene to protect people from serious safety risks – it recognises that safety comes first.

But the Privacy Act is written in general terms (because it has to apply to every kind of organisation, not just in family violence situations). The Privacy Act doesn't always cater for the complexities in the family violence sector. For example, it can be hard in practice to assess how high a risk of family violence is until you put together information from different agencies, with their different perspectives. You might not initially be sure whether the risk is high enough to meet the Privacy Act's "serious risk" threshold for sharing.

The Act's more specific information sharing provisions help to make it clear what you can and can't do.

The permitted purposes cover the areas where those working in the sector **most commonly** need to share information so they can work together to address family violence. It's useful to have a clear list of purposes saying when you're allowed to share, so that you don't have to worry about it every time the question comes up.

The permitted 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.

You must consider whether to share information, but it is not compulsory to share.

You have a duty to consider sharing

If you hold personal information that you reasonably believe is relevant or may be relevant to another agency for one or more of the permitted purposes, then you must consider whether it would be appropriate to share some or all of that information with another person within the sector.

You must consider whether to share information even if:

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

It's particularly important to think carefully about sharing information when it may help protect someone's safety.

The duty to consider sharing can arise in several circumstances, including when:

- another agency or individual in the sector asks you for information
- when you're referring a person to another sector agency for support and assistance
- when you come across evidence of serious safety risks or criminal offending that are relevant to Police, Oranga Tamariki, or other authorities
- when you are unsure how high the risks of family violence are and consulting another agency may make the position clearer.

While you need to consider sharing, nothing in the Act forces you to share personal information.

If you decide not to share information, even though one of the purposes applies, keep a note of why you made that decision.

A. Why is there a duty to consider sharing?

The reason for creating a formal duty to consider sharing is to make sure that people seriously attempt to work together. We need a more effective and integrated system in order to reduce risks of family violence. We also need to reduce the hoops through which people have to jump when they want help – sharing information can make life easier for them.

At the moment, 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).

The Act turns that presumption on its head. If one of the permitted purposes applies, then the starting point is that you *will* share the information. Only then do you consider whether there's a good reason *not* to share the information.

Where sharing personal information will protect a victim or others from a serious risk to their safety, it's very important to consider sharing. Sharing information doesn't necessarily involve disclosing everything that you know about someone. But if you can't keep confidence and keep someone safe from serious harm at the same time, then safety generally takes priority. That's the case under existing law, and professional codes of ethics also allow for it.

Case example

Matthew is eight years old. His teacher, Reana has noticed over the last year that he has become quiet and withdrawn. Over the past month he has struggled to control his emotions and has been aggressive towards the other students in his class.

Reana was at the supermarket yesterday and walked past Matthew's mother, Kate, crying in her car. When Reana asked Kate if she was okay, Kate became distraught. Kate told Reana that her partner Dallas had been using threats against Matthew to blackmail her. During the conversation, it became clear to Reana that Dallas has been using psychological abuse against Kate, and Matthew frequently witnesses this.

Reana is concerned about Matthew and Kate's wellbeing but is unsure what she, as a teacher, can do. She asks one of Matthew's former teachers, Dave, about Matthew and his family. Dave says "everyone knows Dallas takes advantage of Kate's family money".

Psychological and emotional abuse is family violence. As a registered teacher, Reana has a duty to consider sharing the information she now knows about Kate. She should consider asking for Kate's consent to sharing the information but, even without consent, she can contact an NGO that is publicly funded to provide family violence services to investigate further.

However, the comments made by Dave are gossip and irrelevant – she should not share these but may wish to talk to Dave further to establish the accuracy or source of the information as this could be an indication of financial abuse.

B. Why is sharing not compulsory?

Family violence situations are highly variable. Sometimes, sharing information is obviously justified and is the best way to make sure people are safe. Sometimes, it can cause more harm than good.

A decision to share information needs to be made in context, and with proper thought. You need to weigh up the pros and cons, and judge whether it is desirable and appropriate to share personal information in the circumstances. Factors such as what it will take to keep people safe, and how to maintain trusted relationships, will be important. Ultimately, it's your relationship, and your call.

Before making a decision *not* to share, think about whether there's a way to get the best of all worlds. If you're reluctant to share because you don't want to damage a person's trust, talk it over with them. You may be able to show them why sharing will help. Explain who'll

get the information, and how they can help. This might be enough to reassure the person so that they consent to sharing.

Timing can be important too. Someone may be initially unwilling to have information shared, but once you've built an open and trusting relationship, they may be more comfortable with what you propose.

Case example

Greg and his partner Maria live in a small town. Greg has been physically abusing Maria for some months, including recently using strangulation.

Maria asks for advice from Carmen, a local social worker who specialises in helping victims of family violence. Carmen's view is that the level of abuse is escalating. She sees a real risk that Greg may seriously injure or kill Maria.

Carmen explains this to Maria and says that it is important to get the Police involved. Maria is adamant that she does not want to go to the Police. She loves Greg and does not want him to go to prison – she just wants the violence to stop. However, there is no other agency in the area that can take steps to make sure that Maria's safety is protected. Carmen decides to tell the Police.

Carmen is allowed to tell the Police, despite the fact that Maria does not agree to the disclosure.

Carmen should let the Police know that Maria did not want the information to be given to them. The Police will then know to take care with how they approach Maria or Greg. For instance, if Greg thinks Maria reported him to the Police, that could put her at greater risk.

People's safety comes first

Sharing information can sometimes make people **less safe**, rather than safer – most obviously if a victim's information ends up in the hands of a perpetrator who then uses it to contact the victim, or as a tool to harass the victim.

You need to make sure that the information you share, who you share it with, and the way in which you share it are appropriate, and that you don't expose the victim or others to greater harm.

Before sharing information, you must carefully consider whether sharing could create or worsen safety risks for victims.

Information must not be shared:

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

Again, it's not always a question of *whether* information should be shared at all – sometimes it's a question of *how* or *when* it's shared. You may be able to avoid the safety risks if you think things through.

Talk to the victim to find out whether it is safe to share particular information with a specific agency. They may be able to 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.

***For instance**, the victim may know that a member of the perpetrator's family or whānau works at a community organisation. They might have concerns that referring them 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 alternative provider, you may be able to negotiate a process to make sure that the perpetrator's family member will not come into contact with the victim and will not have access to any information about the victim on the computer system. Keep the victim informed. They may then be willing and feel safe to use the service.

Only share relevant information

Only share information where you believe that the information is relevant to one of the permitted purposes.

In particular, the Act does not allow you to:

- share information that other agencies will not be able to use for one of the permitted purposes;
- share too much information – only share the details that are necessary to do the job;
- gossip or be disrespectful about people – stick to the facts and stick to what's genuinely necessary.

A. How can I know what information is relevant?

Your professional experience in the family violence area is likely to give you strong instincts about what's genuinely useful to share.

Formal risk assessment frameworks (such as the Risk Assessment and Management Framework) will also help you figure out what factors are and are not relevant to calculating risks in the family violence area.

In practice, it's often obvious that the information is closely connected with a family violence situation. For instance, relevant information may include:

- details of **what happened** during current or past family violence episodes (eg, Police reports, or statements from participants or witnesses)
- **effects** of family violence on the victims and their whānau (eg, physical harm, or visible or stated distress)
- who else might be **affected** by the family violence (including children or other family members)
- apparent **causes** of family violence, or factors that may **contribute** to the violence or its severity (such as 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
- past **history of services** that relate to family violence, and success (or otherwise) of engagement.

You're likely to be able to quickly identify information that's clearly relevant. 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.

B. Minimise the personal information that you share

It's important only to share the details that are necessary to achieve the purposes that you have in mind. Make sure you know what information is genuinely useful and what is superfluous.

Occasionally, it may even be possible to achieve the permitted purposes by sharing information that does not identify individuals. This can include:

(a) aggregated or statistical information, or
(b) information that has had any identifying information removed.

If it is possible to get to the same place by sharing non-identifying information, then that is what you should do. Using anonymised or de-identified information substantially reduces the chances that people will experience a breach of privacy. Only share personal information when you need to.

You must not use information for personal reasons

If you are authorised to access an agency's systems for your work purposes, 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.

Breaching this rule will amount to acting in bad faith. You will not be protected from liability under your professional codes of ethics, under the Privacy Act, or under other legal rules.

A. Why can't I look up people who I think might be a threat to my family or friends?

You're given access to information on work systems so that you can do your job. That's the only reason you have it. Using information on work-related systems for your own personal motives is a serious breach of trust, privacy and ethical responsibilities. It's almost certainly a breach of your employment (or other) contract, or your obligations of confidentiality. People can and do lose their jobs over inappropriate look-ups.

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.

If you are genuinely worried that someone might be at risk, and that your agency has information that could help, then go through the proper channels. Report the problem to Police, or to other appropriate agencies. Then the information can be shared in the right way and at the right time (including in a way that will protect against conflicts of interest).

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 family violence history.

Consider getting consent, unless unsafe or impractical

You should consider getting the person's consent before sharing their personal information, unless it is impractical or unsafe to do so.

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

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

In particular, you should consider a person's consent as part of the relationship you have with them. You are best placed to determine how to build a trusting relationship with the person and often consent to your actions, including information sharing, is key to this.

A. Where does consent fit in?

Consent isn't the starting point for thinking about information sharing under the Act. The legislation stresses that safety comes first, and thoughts about confidentiality and consent come second.

Situations in which it might well not be practicable or desirable to get consent before sharing, or even to let the person know what you are going to do, include:

- where discussing the situation with the person or trying to get their agreement would create additional serious safety risks, or exacerbate existing risks
- where time is of the essence and you need to share information so you can assess how serious the risk of harm is and what needs to be done to address that harm
- where discussing the situation could jeopardise a Police investigation or a prosecution
- where it is not practicable to contact the person at all, or it is not practicable to contact them safely.

However, consent is very often a foundation stone for **success** and, conversely, failure to get consent may well undermine the purpose for which you are sharing the information.

For example, if you are developing or implementing a plan to work together with other service providers to help the person, you must at least inform the person about what you propose to do (unless there are safety risks) and should try to get their agreement. If they don't want the services, or are not ready to engage, the reasons why are useful to know.

Information sharing can relieve people of the responsibility to make all the arrangements to resolve their situation. It is an excellent tool. However, it should not be used as an excuse to remove people's autonomy, except in circumstances where this is clearly justified.

B. The value of getting consent

Agencies working in the family violence sector have relationships with the people that they help – sometimes long-term relationships. In practice, you will often get better outcomes if you get the consent of the person concerned before sharing their information.

This is because explaining what's happening can be essential to people's willingness to engage with you or with other services. It's vital that people feel safe seeking help and that they will work co-operatively with you. To do that, you need to earn their trust that you'll manage their information properly, share information appropriately, and not expose them to more risk.

Have a conversation with the person about who else you think should have the information about their family violence situation, and why that is going to help them. This includes not only other agencies, but also whānau. That conversation can also alert you to safety risks that you might not have thought about.

Case example

Yesterday, Police were called out to a family violence incident and found Karen seriously injured. Police arrested her partner, Tom.

Sarah works for an NGO that specialises in helping victims of family violence. After being called in by Police and talking to Karen yesterday, she realises that the abuse has been ongoing and is escalating. Sarah sees a real risk that Tom will further injure Karen if he is released on bail, especially if he believes Karen has talked to Police about the specifics of his behaviour.

Sarah is concerned that Police might grant police bail to Tom. Sarah is aware that Karen has said very little to Police because Karen is nervous about Tom finding out. Sarah considers sharing the risk assessment she has developed through her conversation with Karen. She believes it will help Police make an informed decision about bail. Normally she would seek the victim's consent but she cannot get hold of Karen.

Sarah is allowed to share the risk assessment with Police, despite not being able to seek Karen's consent. She should share it as Karen's safety should be her primary concern. Sarah should, however, let Police know that Karen does not know the information has been shared. Sarah should also inform Police of Karen's concern about Tom finding out Police have the information.

Sarah could share the information with Police.

C. Consider telling people before sharing or as soon as possible afterwards

Individuals have the right to ask you what information you have about them and whether you have shared their information. If they ask, or if you share information without discussing it with the individual in advance, you need to let that person know as soon as possible:

- that you have shared the information
- what information you have shared
- why you believed it was necessary to share the information
- who you shared the information with
- what choices the person has about further information sharing
- that they can ask to see the information that you have about them.

However, it may be appropriate not to tell them you have shared information when there is good reason to believe that:

- informing them could create a serious risk to their mental or physical safety
- informing them could create a serious risk to the mental or physical safety of someone else
- disclosing the information could prejudice the ability of the Police to prevent, investigate or prosecute criminal offending.

Additionally, you do not need to inform them if it is not practicable to do so – for example if you can't get hold of them.

D. Why do I need to let people know what I'm doing?

Being open with people about what you are doing and why, is a foundation stone for respect, dignity, and sound, trusted relationships. This makes the person part of the conversation that others are having about them.

Of course, it isn't always possible to let people know what's gone on – for instance, you might not have up-to-date contact details. In some situations, you may create greater risks by telling people what you are doing. However, those situations need to be the exception rather than the rule.

Check that information is fit for purpose

Before sharing personal information, take whatever steps (if any) as are reasonable in the circumstances to check that the information is sufficiently:

(a) accurate
(b) up to date, and
(c) complete.

If you are sharing information that another person will, or may, rely on to make a decision or take action, and you are not sure that the information is accurate, then make that clear to the other agency when you share the information.

If someone thinks that information you hold about them is inaccurate, invite them to state what the correct information should be. Then either:

(a) correct the information that you hold; or
(b) attach a note (a "statement of correction") to that information stating what the person thinks the correct facts are (so that the person's view can be considered whenever the information is used).

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

A. How accurate is 'accurate'?

Factors that affect whether information is sufficiently accurate, up to date, or fit for purpose 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, a decision about what services would be appropriate, or how to provide those services
- whether the information is negative, or may be seen as negative, about an individual.

Reasonable steps to check the information may include:

- discussing the information with the individual
- cross-checking the information with another agency or individual in the sector
- 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 wrong. You're not required to categorically guarantee that information is right before you pass it on. You just need to take reasonable care.

What is "sufficiently" accurate, up to date or complete depends on the purpose for which it is to be used.

Sometimes, the accuracy of information may not be particularly important – it's the job of the agency that's receiving it to work out whether the information is right or not.

> ***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: they 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 perpetrator might have reoffended or is about to reoffend, you can talk to the Police. It's up to the Police to decide whether to make further enquiries.*

Conversely, 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 is negative – that is, it could create trouble for someone when you share it – it's particularly important to make sure it's as correct 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 (including photos, if they are available) to make sure you've got it right.

Record reasons for decisions

If you receive a request from an agency to share personal information that is or may be relevant for one of the permitted purposes:

(a) keep a record of the request
(b) note whether or not your agency agrees to the request, and the reasons for that decision
(c) if you decide to agree to the request, note what information was sent and when it was sent.

Equally, if you request personal information from another agency:

(a) keep a record of the request, including what you wanted and why you wanted it
(b) note who you spoke to.

If you decide to disclose information proactively to another agency (that is, you decide you should send it without receiving a request):

(a) note why you believe that disclosing the information would fit with one of the permitted purposes
(b) note what information was sent and when it was sent.

A. I'm really busy and keeping notes is a pain – do I have to?

Keeping records of your decisions doesn't need to involve bureaucratic or resource-intensive filing. Brief notes will do.

Just make sure that you include the dates when things happened, what was decided, and who made the call.

If you have level 2 Ministry of Social Development accreditation, you should use the system you have in place to deal with privacy requests.

If you're sending an email or a letter, you're most of the way there. Just put it in the client file.

If you've shared information over a telephone call and you can't type straight into the client file, at least make handwritten notes of what was said and add them to the client file later (either put them in a physical file, scan them in to an electronic system, or type them in when you're doing your admin).

Record keeping is important for a number of reasons. It will help you explain what you've done, and why, to the person whose information you've shared, if they ask you (and to the Privacy Commissioner or your professional organisation). It will also help your agency look back at what information has been shared in the past and make more consistent decisions about when it believes it's appropriate to share information.

Protection from liability for sharing

If you share information in accordance with the rules under the Act, and follow this guidance, then you will not be legally liable, unless you were acting in bad faith. However, there are some rules that still prohibit information sharing, outlined below.

For example, if someone complains that you have breached their privacy, breached confidence, or breached your professional ethical obligations, then that complaint will not be upheld as long as you've complied with the Act. It doesn't stop someone from *making* a complaint, but it does provide you with legal protection.

The law provides this protection so you do not need to be unduly concerned about sharing information when you genuinely think that sharing is necessary to help people involved in a family violence situation.

The only exception is where you have shared the information in bad faith. Bad faith usually arises where someone has malicious or ulterior motives, or acts with intent to deceive. Where people are so grossly careless that it appears they have made no attempt to comply with their legal obligations, this might also be seen as amounting to bad faith.

Provided that you do not act in bad faith, you will not breach the professional codes of ethics that relate to health professionals, teachers and social workers.

The Act doesn't force you to share information, and it is not the only information sharing mechanism that may be relevant to you or to the particular family violence situation.

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, then provide the information that is covered by that warrant or order.
- 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 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).

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

For example, section 66 of the Oranga Tamariki Act allows Oranga Tamariki to demand information from other government departments and statutory bodies. There are limits on what the information can be used for. Section 66, as it stands, does not enable Oranga Tamariki to demand information from NGOs.

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 order what is required.

B. What happens in the context of mandated family violence programmes?

The Act contains some specific provisions that govern what happens when the court orders perpetrators (respondents) to attend risk assessment and programmes.

If you are a risk assessor or service provider, make sure that you are familiar with your obligations to provide information back to the Court and other authorities in certain circumstances. Check the code of practice that governs court-directed assessments and programmes for further details.

If you are a risk assessor or service provider and have concerns about the safety of a protected person (that is, concerns that go beyond the reasons provided for the protection order, and that appear to be imminent, escalating or grave), you must without delay, notify:

- the Registrar of the Court, and
- the District Commander at the appropriate Police District Headquarters (which can be by calling 111), and
- if there's a perceived risk to any child, Oranga Tamariki.

The Registrar then has to arrange for the protected person to be notified of the concerns, and refer the matter to a Judge, or take steps to call the respondent before the Court.

These referrals can sometimes create difficulties for protected people, as the Court may decide the perpetrator needs to receive information in order to be able to answer allegations against them. While you still have to disclose your safety concerns, alert the Registrar, Police or Oranga Tamariki to any specific concerns that you may have so that they are aware of the sensitivities involved and can discuss the matter with the protected person.

C. Know what information you're not allowed to share

Sometimes, other statutes will prohibit information sharing. Again, you don't need to worry about the Privacy Act if you're sharing under the Act, but other rules will apply as normal. 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) Court information

Information that is under the control of the courts is governed by the court rules. It isn't Ministry of Justice information – the Ministry's role is to manage the information for the court, and it doesn't hold the information for its own purposes.

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

General rules on court records are set out in the District Court Act and the Senior Courts Act. The Act doesn't affect them.

(b) Privileged information

If the information is covered by legal privilege, religious privilege, medical privilege or journalistic privilege, it is protected in the normal way under the Evidence Act.

Similarly, the right against self-incrimination remains in place.

Part III: Store information safely

A. Only keep information for as long as necessary

If you're not confident that you can still use the information for the purpose for which you got it, then you should:

(a) securely delete or destroy that personal information; or
(b) remove or disguise all the identifying details, so that someone reading it would no longer be able to pick out who the individual people are; or
(c) strip the information back to statistics rather than individual records.

Only keep personal information beyond that time if:

(a) another law requires you to (for example tax legislation, the Public Records Act 2005, or the Health (Retention of Health Information) Regulations 1996)
(b) you're obliged to keep the information under a contract (such as a contract with a family violence funding agency) or under ethical rules
(c) you believe that there is a risk that the family violence situation may recur and that you may need to supply the information to another agency in future.

B. Why do I need to think about deleting personal information?

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 hang onto 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. You just need to think about it.

For instance:

- Some agencies may be dealing with their family violence clients for a long time. The clients may come and go. You won't want to start from scratch if you're reasonably confident they could come back through the door and you need to know what's happened previously. When they do come back make sure you update your records.
- Some (particularly the statutory agencies) have ongoing legal obligations, or sound public policy reasons, to keep information for a long time. For example, the Public Records Act may apply. Police need to maintain criminal history records, and Oranga Tamariki need to keep child welfare records.
- If you're a health agency, you need to hold on to health information in accordance with the Health (Retention of Health Information) Regulations, for a period of 10 years. Tax records need to be kept for 7 years.
- Some contracts will also spell out how long you need to keep information for.

But most of us don't need to hold on to information forever. It takes up space and creates problems if it gets lost or misused.

For example, you may have information about all your past clients on your system. Think about what you'd do with it. If the answer is 'nothing', and there's nothing stopping you from deleting it, then that's usually the way to go.

If the information came from another agency in the first place (for example a Police report), then the original agency is likely to hold the authoritative copy of that information. It's far less likely that you also need to hold onto it. If someone else needs it, it will still be available.

Your own records that you've created when dealing with the victim or perpetrator, or their family or whānau may be different – it's harder to reconstitute those if you need to refer to them later, so you need to think more carefully.

The question is whether you'd ever use that information again for the reason you got it. If the answer is no, or if you could achieve the same end by using de-identified information or statistical information, then delete it or protect your clients by reducing it to non-personal information.

When working out how long you need to keep information, remember that if you keep it, you're responsible for keeping it safe.

C. Make sure information is kept safe when sharing

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.

D. Particular steps to ensure safety of information

Make sure the information does not get lost, misused or sent to the wrong place. For instance:

(a) check physical or electronic addresses,
(b) make sure you're giving the right information to the right person,
(c) make sure your staff all know the rules about what can be done with the information and how to make sure it's treated properly.

Set up safe communication channels, so that the information does not get intercepted or end up in the wrong hands. For instance:

(a) Remember that email is not particularly secure – be careful what you use it for. Encrypted channels, like virtual private networks (VPNs) are good if you can use them.
(b) Beware of putting sensitive client information into free online file sharing systems – they aren't always secure, and most are governed by foreign laws so it can be hard to fix problems if they arise.
(c) It's not ideal to share information on memory sticks, or other portable media, but if you have to, then make sure that they are encrypted and that you have strict processes to make sure they don't get lost or stolen.

Make sure only relevant and authorised people have access to the information that you store. You should:

(a) lock paper records away – don't leave them where anyone could see them
(b) keep paper records out of public areas of your building (such as places where you meet other clients), and make sure the public can't see information about other people on your computer screens
(c) protect paper printouts of family violence incidents, or other client records, particularly when away from the office – they are easy to lose or drop
(d) use secure bins or shredders to dispose of paper records
(e) check who has access to your computer systems and, where possible, lock certain files so that only authorised people can see them
(f) make sure there are rules in place for employees or contractors, to make sure they keep information confidential, that they know what information they're allowed to access and what they're allowed to do with it
(g) take basic security steps such as:
    - making sure you have password protection on all devices that may contain client information (like laptops and phones)
    - check passwords are strong
    - keep computer firewalls and antivirus up to date
    - watch out for scam emails that may install viruses on your computers and train your staff to spot them
    - include a signature on emails that asks people to delete the information and let you know if they receive the email in error.

E. Security stuff is technical – who can I ask for help?

You don't have to be a computer expert to get security right. 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)

F. Manage privacy breaches appropriately

If you discover that a privacy incident has occurred – that is, 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, ensure that it is deleted, and ensure that it is not further disclosed
- notify any agency that was the source of the information
- notify the Privacy Commissioner if there is a possibility that the breach could cause harm to someone
- decide whether to notify any individual whose information has been compromised by the incident, if necessary after consulting with the source agency and the Privacy Commissioner, and
- assess how the incident occurred, and take whatever steps are reasonable to prevent such an incident from happening in future.

G. Is it compulsory to notify people about breaches?

The current Privacy Act doesn't include a requirement to notify the Privacy Commissioner or individuals about privacy breaches. However, mandatory notification will come into law as part of the new Privacy Act when it is passed by Parliament.

In the meantime, notification is good practice, particularly as family violence information is often highly sensitive and it is important to deal with any breaches responsibly.

H. When do I have to notify the person or people whose information is involved?

There are relevant factors that can be taken into account when deciding whether to notify an affected individual.

You should notify the person or people if:

- notifying the individual could enable them to take steps to protect themselves from significant harm (you should almost invariably notify in such circumstances);
- the breach affects a large number of people
- the breach involves particularly sensitive information.

However, it may be appropriate not to notify the person or people if:

- the information has been sent to someone who has returned or destroyed it or who can be trusted not to misuse it
- the information was in a form that means it's protected despite potentially being in the wrong hands (for example when it's encrypted)
- notifying the individual could cause disproportionate harm or distress to them (for instance where there isn't a high risk of harm, but the person's mental health could

be seriously affected by a notification and you can't address that by notifying them in a particular way)
- letting the person know could compromise a criminal investigation.

It's important to notify people in the right way:
- make sure that when you contact them, you can explain clearly what information was involved, what happened and what you are doing about it
- if you're not sure exactly what happened yet, make arrangements to keep them updated
- give them your contact details, or contact details for someone else in the organisation that they can talk to about any concerns they have
- tell them they can talk to the Privacy Commissioner's office
- if you can think of steps that they could take to prevent any harm from occurring, then make those suggestions
- if, in the worst case scenario, the incident has created a serious risk of harm to them, then contact people who can help to manage the risk (such as Police), and work with the person to come up with a plan to keep them safe (for instance, if a victim's confidential address has been leaked to the perpetrator or their associates, the plan might have to include relocation).

If you don't know who has been affected by a breach, or you can't contact them individually, you may need to put information onto a website, or use another public form of communication.

Again, make sure you're clear about what's happened and what kind of information is involved. You need to be honest, but don't scare people unnecessarily. For example, don't suggest that whole medical files have been lost when the worst-case scenario is that it's only people's names and email addresses that are involved. That might still be a problem – but it's a different problem.

For more advice, the Privacy Commissioner's office has an excellent data safety toolkit available on its website at: https://www.privacy.org.nz/data-breaches/data-safety-toolkit/.

Part IV: Provide access to personal information

A. The right to access information

Under principle 6 of the Privacy Act (and rule 6 of the Health Information Privacy Code 1994), people have a right to both

- seek confirmation that an agency holds their personal information, and
- ask agencies for access to that personal information

The Act does not affect this right, so you need to comply with the law in the usual way.

However, the Privacy Act does not give people a right to ask for access to information that's purely about other people.

B. Why do people have a right to access information about themselves?

A core aspect of the Privacy Act is that people should have the ability to see what information an agency holds about them. Access to their personal information means they can see what others know about them and whether the agency acted properly (and challenge a decision if they believe the agency acted improperly).

They can check whether the information is correct, so any mistakes can be quickly fixed or disagreements about facts can be noted. These are also entitlements under principle 7 of the Privacy Act.

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.

C. When can I say no?

There will sometimes be good reason to refuse an access request, or to delete some of the information that's been requested. Those reasons are all listed in the Privacy Act (or Health Information Privacy Code) or are contained in other legislation. If your reason is not on the list, you can't refuse a request.

In the context of family violence, key reasons to refuse requests can include:

- Protecting someone's safety – most obviously where revealing information to a perpetrator might create or increase a risk of harm to the victim (such as disclosing a

victim's new address or contact details, or revealing that they are about to leave a relationship) (section 27(1)(d)).
- There's an ongoing criminal investigation, and disclosing the information could get in the way of that investigation or the potential for a successful prosecution (section 27(1)(c)) – check with the Police if you are unsure whether providing the information could raise these risks.
- Releasing the information would be contrary to the interests of a child (section 29(1)(d)).
- Disclosing the information would mean unjustifiably breaching someone else's privacy – for example, causing a risk of harassment, breaching their confidence, or exposing information that is personal or sensitive (section 29(1)(a)).
- Disclosing the information could jeopardise someone's mental health – a decision on this ground should have the support of a health professional who's familiar with the person concerned (section 29(1)(c)).
- Copies of victim impact statements must not be provided to the offender (section 23 (4) of the Victims' Rights Act 2002).

D. What to do when you get an access request

You must:
- **find** all the information that the person has requested
- if you don't hold any information – and you don't think another agency has it – then you can say so, and decline the request (but bad record keeping is not an excuse)
- if you think another agency has the information (or it's their information rather than yours), first **check** with that agency and **transfer** the request to them within 10 working days. Tell the requester what you've done.
- **consider** whether to provide the information or whether there is a good reason under the Privacy Act to decline the request – make sure this is done by someone familiar with the Privacy Act, so you get it right
- **tell the person** whether you have decided to grant the request as soon as practicable (but no later than 20 working days after receiving the request)
- if the decision is to **agree** to provide access, then provide that access – for instance, by providing a copy of documents – **without undue delay.**

If you decide to refuse to provide any or all of the information, **state** which of the Privacy Act grounds for refusal apply, and tell the person that they can **complain** to the Privacy Commissioner if they think the decision is wrong.

Before giving the requester the information:
- make sure that you're giving it to the **right person** (it's not unheard of for people to pretend to be someone else in order to get access to information, for example an associate of a perpetrator might pretend to be the victim)
- check it's going to reach that person safely and isn't likely to be intercepted (for instance, arrange a safe place for collection).

E. Keep a record of the request and the information you send

Make sure you keep good records. Keep copies of:

- the request (including when you received it)
- your response (including when you sent it)
- a copy of all the information you sent to the requester
- if you deleted or redacted any information, then a clean copy of any documents where those deletions or redactions were made.

F. Why do I have to keep copies of stuff that I send to requesters?

More than half of all complaints that go to the Privacy Commissioner are about what agencies have done with access requests. It isn't common for those complaints to deal with family violence situations but it can happen. If there is a complaint, you need to be able to show what you did and why. If you don't have records, you won't be able to do that.

It's also useful in case the person makes other requests in the future. At the moment, there's nothing in the Privacy Act that stops people from making repeat requests (as long as they're not doing so simply to be a nuisance) and the reality is that people sometimes lose information and need fresh copies. If you have a copy of the information you've already provided, this will make it a lot easier to re-send it in the future. All you'll need to do is think about whether the circumstances have changed – for instance, whether there's no longer a reason to withhold the information.

G. Charging

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, it's probably not worth the hassle, particularly if you are dealing with someone who needs the information but doesn't have any money.

Part V: Collect information appropriately

A. Purpose for collecting personal information

You can collect personal information related to family violence when it is necessary for your role. Under the Privacy Act, personal information can be collected by an agency if the information is collected for a lawful purpose connected with a function or activity of the agency and collection is necessary for that purpose.

An agency does not need to show that it absolutely must collect the information in order to achieve its purpose. But it does have to show that it is reasonably necessary to collect it.

In order to make sure you only collect the information you need, you should have a clear idea of what you want to be able to do with the information. In other words, you need to know what your purpose is for collecting personal information before you collect it, rather than gathering a large amount of personal information on the off-chance you might need it for something.

The government agencies in the family violence sector will often be operating under their own statute, which may provide another statutory basis for information collection.

B. Personal information should be collected directly from the person

Generally, you should collect personal information directly from the person concerned. This will help ensure the information is accurate and up-to-date.

Collecting information from the person concerned also means that people know what is going on and have some control over their information.

However, there can be situations where it's not appropriate or possible for you to collect information directly from the person concerned. The Privacy Act contains a range of exceptions to deal with these situations, including if the information is publicly available or the individual concerned has authorised collection from someone else.

The Act's information sharing provisions are an additional exception. You can request information from another agency or individual in the sector for one of the permitted purposes, rather than collecting directly from the person concerned.


Collecting Information

C. How information should be collected

Information should not be collected by unlawful means, in a way that is unfair or in a manner that is unreasonably intrusive. For example, it's an offence to record a phone conversation unless you're a party to the conversation.

D. Tell the person that you are collecting information about them

When you collect personal information directly from a person, you should take reasonable steps to ensure the person is aware that you are collecting the information. What the reasonable steps are will depend on the circumstances of the particular case.

In most cases, the person will be a client and collecting personal information from them is part of your role and well understood. However, you should also take reasonable steps to let the person know:

- the reason you are collecting the information and any intended recipients
- the name and address of the agency collecting or holding the information
- which law applies and what is required of the person under the legislation
- their rights to access and correct personal information under the Privacy Act.

You should let the person know all of this before information is collected or as soon as practicable after collection. This avoids surprise down the track about how the information is used or who it has been given to. It enables them to have a voice, and to participate to the extent that is possible for them. 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.

Case example

Margaret is in her eighties and suffers from dementia. Her son Wiremu has recently moved her to a rest home so she can get the support she needs.

Wiremu gets in touch with an NGO that provides government-funded family violence services through its helpline. Tess works at the NGO and talks with Wiremu, who tells Tess that his sister, Miriama, has been using emotional abuse to "win his mother over". Wiremu says Miriama has told Margaret that Wiremu has abandoned her when he "left her alone in a home", causing Margaret emotional distress.

Tess informs Wiremu that the situation may amount to family violence and he can seek a protection order on behalf of Margaret.

Tess should also inform Wiremu that she has written a case note about the situation, including details about Margaret. While it might not be appropriate for Tess to inform Margaret that she is collecting personal information (this might cause further distress and confusion given Margaret's mental state), Tess should tell Wiremu what information she is collecting and who it might be shared with.

Ministry of Justice
Tāhū o te Ture

justice.govt.nz

info@justice.govt.nz

0800 COURTS
0800 268 787

National Office
Justice Centre | 19 Aitken St
DX SX10088 | Wellington | New Zealand

New Zealand Government

Reference no_March16