SUMMARY OF THE FAMILY VIOLENCE INFORMATION SHARING GUIDELINES

Guidance for
Information Sharing Entities

family safety victoria

VICTORIA
State Government

Introduction

The Royal Commission into Family Violence (the Royal Commission) found that effective and appropriate sharing of information is crucial in keeping victim survivors safe and holding perpetrators to account. The Royal Commission also identified a number of barriers in Victoria that prevent effective information sharing and the potentially catastrophic consequences of not sharing information.

The Victorian Government adopted the Royal Commission's recommendation and established a family violence specific information sharing scheme in Victoria under Part 5A of the *Family Violence Protection Act 2008* (FVPA), which commenced on 26 February 2018. The Family Violence Information Sharing Scheme (the Scheme) broadens the authorised information sharing environment for two main aims: to ensure the safety and protection of those experiencing family violence; and to hold perpetrators to account. The Scheme authorises a select group of prescribed information sharing entities (ISEs) to share information between themselves for family violence risk assessment and risk management.

A new Child Information Sharing scheme (CIS scheme) established by the *Child Wellbeing and Safety Act 2005* commences on 27 September 2018. ISEs must also consider whether information held by the ISE should be shared to promote the broader wellbeing or safety of a child under the CIS scheme. Chapter 3 of the Child Information Sharing Guidelines <https://www.vic.gov.au/infosharing/resources.html> provides information on the intersection of the two information sharing schemes. This summary of the Family Violence Information Sharing Guidelines (Guidelines) explains how to share information under the Scheme. For more detailed information please see the Guidelines.

The family violence information sharing scheme

How information can be shared under Part 5A

ISEs are prescribed by regulation and are required to comply with Part 5A. Any personal, health or sensitive information that is relevant to assessing and/or managing family violence risk can be shared between ISEs, provided:

- the information is not excluded
- sharing the information does not contravene another law, and
- applicable consent requirements have been met.

The information may relate to a victim survivor (adult or child), an alleged perpetrator or perpetrator, or third party.

Information can be shared verbally or in writing.

Where an ISE receives a request, it **must** share that information, provided that the information meets the requirements of the Scheme.

An ISE should always prioritise requests for information under Part 5A and respond to requests in a timely manner. In particular, where a serious threat has been identified, ISEs should respond to those requests for information without delay.

Purpose of sharing

There are two purposes for which information can be shared between ISEs under Part 5A:

- **Family violence assessment purpose:** to establish whether family violence risk is present, assessing the level of risk the perpetrator poses to the victim survivor, and correctly identifying the perpetrator and victim survivor
- **Family violence protection purpose:** once family violence risk is established, to manage the risk of the perpetrator committing family violence, or the risk of the victim survivor(s) being subjected to family violence. Managing risk involves removing, reducing or preventing the escalation of risk. This includes information sharing to support ongoing risk assessment.

All ISEs will be able to share information for a family violence **protection** purpose. ISEs that are also prescribed as risk assessment entities (RAEs) can also share information for a family violence **assessment** purpose.

An ISE may also share perpetrator information with a victim survivor if the ISE reasonably believes the information will assist the victim survivor to manage their safety or their children's safety. The ISE should ensure that a victim survivor knows that they can only use the information to manage their safety or that of their children, not for any other purpose.

Relevance and reasonable belief

Before sharing relevant information with an RAE for an **assessment purpose**, an ISE does **not** need to hold a reasonable belief that the disclosure is necessary for a family violence assessment.

This is distinct from sharing relevant information for a **protection purpose**, where an ISE must hold a reasonable belief that the sharing is **necessary** for a protection purpose. This supports proportionality, to ensure that sharing of information is done only to the extent that it is relevant and necessary for management (including ongoing assessment) of family violence risk.

Definition of a victim survivor, alleged perpetrator or a perpetrator in Part 5A

Alleged perpetrator

A person may be an alleged perpetrator where the ISE has limited information but there is a suspicion that the person poses a risk of committing family violence.

ISEs can only share information about alleged perpetrators with RAEs for a family violence **assessment purpose**, using a family violence risk assessment based on the Family Violence Multi-agency Risk Assessment and Risk Management Framework (the MARAM Framework) to establish if the person is a perpetrator and assess the level of risk they pose.

Perpetrator

A person is a perpetrator if an ISE reasonably believes that there is a risk that the person may commit family violence. This may have been identified through undertaking a MARAM Framework-based family violence risk assessment. This is the same meaning as a '**person of concern**' in Part 5A of the FVPA.

Information about perpetrators may be shared with any ISEs for a family violence **protection purpose** (including ongoing risk assessment).

Victim survivor

Victim survivor has the same meaning as a '**primary person'** as defined in the FVPA. A person will be a victim survivor (adult or child) if an ISE reasonably believes there is risk that the person may be subjected to family violence.

Third party

A third party (or **linked person**, under the FVPA) is any person whose confidential information is relevant to assessing or managing family violence risk who is not a victim survivor, perpetrator or alleged perpetrator. This could include previous partners of either party, friends, acquaintances, neighbours or associates of a victim survivor, perpetrator or alleged perpetrator.

Consent Thresholds

The Family Violence Information Sharing Scheme prioritises:

- a child's safety over any individual's privacy
- victim survivor safety over perpetrator privacy.

The Scheme also promotes a timely whole of system response to holding perpetrators to account.

No consent required

Consent is **not required** from an alleged perpetrator (for an**assessment purpose**) or a perpetrator (for an **assessment purpose** or **protection purpose**), including adolescents who use violence in the home, when sharing information under Part 5A to assess or manage risk of family violence to a child or adult victim survivor.

Consent is **not required** to share relevant information about **any person** when assessing or managing risk to a **child victim survivor** of family violence (a person who is under 18 years of age). ISEs should take all reasonable steps to seek and obtain the views of the child and/or any parent (who is not a perpetrator) when sharing their information when consent is not required, and to take those views into account where it is safe, appropriate and reasonable to do so.

Consent required

When sharing information about:

- An adult victim survivor (where there are no associated children at risk of family violence): **Consent is required** to share relevant information about an adult victim survivor, unless the ISE reasonably believes that sharing information is necessary to lessen or prevent a **serious threat** to an individual's life, health, safety or welfare
- A relevant third party: **Consent is required** to share information about a third party, unless the ISE reasonably believes that sharing confidential information is necessary to lessen or prevent a **serious threat** to an individual's life, health, safety or welfare. Relevant third party information may also be shared without consent if de-identified.

Exceptions to information sharing

Information is excluded and should not be shared under the Scheme if, given the facts known to the worker, sharing that information could be reasonably expected to:

- endanger a person's life or result in physical injury
- prejudice the investigation of a breach or possible breach of the law or the enforcement or proper administration of the law in a particular instance
- prejudice a coronial inquest or inquiry or the fair trial of a person or the impartial adjudication of a particular case
- disclose the contents of a document or a communication that would be privileged from production in legal proceedings on the ground of legal professional privilege or client legal privilege
- disclose, or enable a person to ascertain, the identity of a confidential source of information in relation to the enforcement or administration of the law
- contravene a court order or law that prohibits or restricts, or authorises a court or tribunal to prohibit or restrict, the publication or other disclosure of information for or in connection with any proceeding
- contravene a court order or law that requires or authorises a court or tribunal to close any proceeding to the public
- be contrary to the public interest.

It may be necessary for an ISE to obtain legal advice to determine if any of these exemptions apply.

Any refusal to share on the basis that the information is excluded must be provided in writing, with reasons stated. Where it would be inappropriate to provide details of the specific ground for the exclusion, it is sufficient to refuse on the grounds that the information is excluded.

If a person decides that information is not excluded, but the result of sharing the information results in one of the above outcomes, that person will be protected from any consequences of their decisions provided they were acting in good faith and with reasonable care.

Accountability for ISEs

If information is shared inappropriately under Part 5A, offences may apply and penalties may be imposed. However, if the person sharing the information acted in good faith and with reasonable care they will not be held liable in relation to the use or disclosure of information.

ISEs should ensure that they have appropriate processes in place to guard against privacy breaches. This includes taking steps to ensure that perpetrators cannot access information about a victim survivor and that workers requesting information or working with a client do not have a conflict of interest. For further information see Chapter 1 — Family Violence Information Sharing Scheme <https://www.vic.gov.au/familyviolence/family-safety-victoria/information-sharing-and-risk-management/resources.html>.

Figure 1:
Overview of the Scheme

WHO CAN SHARE

Information sharing entities (ISEs) are authorised to share information. These ISEs are:

- Prescribed by regulations

WHY THEY CAN SHARE

Relevant information about a person (adult or child) who is a victim survivor, perpetrator or a third party can be shared for the purpose of:

- Establishing and assessing risk
- Managing risk

WHEN CAN THEY SHARE

ISEs can share information:

- Voluntarily with other ISEs
- In response to a request from another ISE

WHAT CANNOT BE SHARED

- Excluded information (including but not limited to) if sharing the information might endanger a person's life or result in physical injury, prejudice legal proceedings or a police investigation, contravene a court order, or is subject to legal professional privilege
- ISEs cannot share information that would contravene another law that has not been specifically overridden by the scheme

Adult Victim Survivor An ISE reasonably believes that there is a risk that the person may be subjected to family violence	→	**CONSENT REQUIRED** from the adult victim survivor prior to sharing their information unless there is a serious threat or the information relates to assessing or managing a risk to a child victim survivor (no consent - see below)
Child Victim Survivor An ISE reasonably believes that there is a risk that the person (under the age of 18 years) may be subjected to family violence	→	NO CONSENT REQUIRED from any person if their information is relevant to assessing or managing risk of family violence to a child victim survivor
Perpetrator An ISE reasonably believes that there is a risk that the person may commit family violence	→	NO CONSENT REQUIRED from the perpetrator prior to sharing their information to assess or manage risk of committing family violence
Alleged Perpetrator A person who is alleged to pose a risk of family violence **Note:** information about an alleged perpetrator can only be shared in the risk assessment phase	→	NO CONSENT REQUIRED from the alleged perpetrator prior to sharing their information to establish or assess risk of committing family violence
Third Party A person whose information is relevant to assessing or managing a risk of family violence	→	**CONSENT REQUIRED** from the third party prior to sharing their information unless there is a serious threat or the information relates to assessing or managing a risk to a child victim survivor (no consent - see above).

All ISEs **must respond to information requests** unless an exemption applies

A good faith defence protects individuals who share information in good faith and with reasonable care

The **scheme will be reviewed** after 2 years, and then again after 5 years

Complaints about privacy breaches can be made to the Victorian Information Commissioner or the Health Complaints Commissioner

Information sharing entities

Information sharing entities under Part 5A

ISEs authorised to share information under Part 5A are prescribed in the Family Violence Protection (Information Sharing and Risk Management) Regulations 2018.

Risk assessment entities (RAEs) are a subset of ISEs that can request, collect and use information for a **family violence assessment purpose**, to establish and assess risk at the outset.

Once initial risk has been established, all ISEs are permitted to request, collect, use and disclose information for a **family violence protection purpose**, which includes the ongoing assessment and management of an established risk.

See Chapter 2 — Information sharing entities for a list of currently prescribed ISEs.

Sharing information about perpetrators and alleged perpetrators of family violence

Collecting and sharing information about alleged perpetrators/ perpetrators

When an ISE collects information **directly** from a perpetrator or alleged perpetrator, the perpetrator or alleged perpetrator should be informed of how their information may be used or disclosed under Part 5A.

This should occur at or before their engagement with the ISE.

Where their information has been has been collected **indirectly** about a perpetrator or an alleged perpetrator (for example, from the victim survivor or from another ISE), ISEs are not obliged to notify the perpetrator or alleged perpetrator.

Consent is not required to share relevant information about an alleged perpetrator or a perpetrator.

Determining whether a person is a perpetrator or a victim survivor

In some circumstances, an ISE may have difficulty in determining who is a victim survivor of family violence and who is perpetrating family violence. For example, each adult in a relationship might claim that their partner is the perpetrator.

A person can be considered a perpetrator if an ISE reasonably believes that there is a risk that the person may commit family violence (described as a 'person of concern' in Part 5A).

A MARAM Framework-based risk assessment should be used to decide whether there is a risk that a person may commit family violence. The MARAM Framework should be used to identify a perpetrator of family violence towards both an adult and child victim survivor.

ISEs should be cautious about sharing information in response to a request when there is any suspicion the perpetrator has been misidentified. ISEs should be particularly careful about incorrectly identifying a perpetrator when the person has previously been identified as the victim survivor of family violence or where both parties claim to be the victim survivor.

An ISE may receive a request to share information about a person that they believe has been incorrectly identified as a perpetrator or a victim survivor. When this happens, an ISE should raise their concerns with the requesting ISE, citing any relevant considerations from the MARAM Framework.

If there continues to be conflicting assessment between ISEs about who the perpetrator or victim survivor is, ISEs should only share information about that person in accordance with their assessment of each person's identity and apply the relevant consent thresholds. ISEs should have policies and procedures in place to assist with resolving differences of professional opinion and disputes with other services about identifying the perpetrator and victim survivor.

For example, where an ISE has requested information about a person it has assessed to be a perpetrator, and the responding ISE has assessed that person to be a victim survivor, the responding ISE can only share that person's information in accordance with the general rules for sharing a victim survivor's information. It should inform the requesting ISE that they have assessed the person to be the victim survivor and will only share the information with the consent of the person. Unless consent is provided, the responding ISE would not be authorised to share the person's information. This is the case regardless of the fact that the requesting ISE has assessed the person to be a perpetrator.

Correcting errors

Where it is established that a person has been incorrectly identified as a perpetrator, an ISE must stop sharing information about that person, make a written record of why information sharing has been stopped, and keep this record on file. Information about the person can continue to be shared in accordance with Victorian privacy laws or the applicable Part 5A thresholds.

The ISE should make best effort to correct the information that has already been disclosed, and update relevant records. The correction of records should occur in a timely manner. An ISE may also choose to notify a person that their information was shared without their consent.

See Chapter 3 — Sharing information about perpetrators and alleged perpetrators of family violence for more information.

Sharing information to assess and/or manage risks to an adult victim survivor

Adult victim survivor information

ISEs must obtain the consent of an adult victim survivor before sharing their information to assess or manage their risk, unless:

- the ISE reasonably believes that the sharing is necessary to lessen or prevent a **serious threat** to a person's life, health, safety or welfare, or
- the information is also relevant to assessing or managing a risk of family violence to a child.

ISEs should only share relevant information and handle the information in a secure way according to the existing obligations under the *Privacy and Data Protection Act 2014* (PDP Act) or the *Health Records Act 2001* (HR Act).

When sharing information without consent, an ISE must make a professional judgement about whether the ISE has the legal authority to disclose the information under Part 5A or another Act. When making a decision about whether to share information without consent, an ISE should comply with their organisation's protocols, policies and service standards. Refer to Chapter 4 for further information.

ISEs should involve victim survivors in the process to ensure that they understand that only information that is necessary to prevent or lessen the serious threat will be shared, and the potential outcomes of sharing that information. Refer to Chapter 10 for information about what records need to be kept when sharing information under Part 5A.

Third party information

A third party (defined in the legislation as a linked person) is any person who is not a victim survivor or perpetrator whose information is relevant to assessing or managing a risk of family violence. Consent is required to share information about a third party when assessing or managing risk for an adult victim survivor, unless the ISE reasonably believes that the sharing is necessary to lessen or prevent a serious threat to a person's life, health, safety or welfare. Consent is not required when sharing third party information to assess or manage risk to a child victim survivor.

ISEs can share information about a third party in a de-identifiable way without their consent. However, a person's right to privacy should be displaced only to the extent that is necessary to assess and manage a risk of family violence.

For further information see Chapter 4 — Sharing information about adult victim survivors or third parties to assess and/or manage risks to an adult victim survivor.

Assessing and managing risks for a child victim survivor

How does Part 5A interact with the Child Protection system?

- An ISE's existing mandatory reporting obligations to Child Protection continue to apply.
- Nothing in Part 5A impacts on information sharing already permitted under the *Children, Youth and Families Act 2005* (CYFA).
- Part 5A may be used to share information between ISEs (including Child Protection and Child FIRST, once prescribed).

The interaction between Part 5A and the CIS scheme

In addition to family violence risk, ISEs assessing and managing family violence risk must also consider the broader wellbeing and safety concerns of children engaged with their service.

ISEs prescribed under both Part 5A and the CIS scheme are able to share information under the CIS scheme to address child wellbeing and safety issues in addition to family violence. For example, as well as assessing and managing family violence risk for a particular child using information obtained under Part 5A, information should also be safely shared under the CIS Scheme, in accordance with the child's family violence safety plan, to promote their wellbeing by accessing appropriate educational support for learning difficulties.

Chapter 3 of the CIS Guidelines <https://www.vic.gov.au/infosharing/resources.html> provides guidance on sharing information under the CIS scheme to promote the wellbeing or safety of a child when family violence is present.

Consent requirements

Under Part 5A, a child's safety from family violence is prioritised over any individual's privacy. Accordingly, anyone's information (including the child and their victim survivor parent, an alleged perpetrator, a perpetrator, or any third party) can be shared without their consent if that information is relevant to assessing or managing a risk of family violence to a child (defined as a person under 18 years).

However, ISEs are encouraged to take all reasonable steps to seek and obtain the views of the child and/or parent (who is not a perpetrator) and to take those views into account where it is safe, appropriate and reasonable to do so.

The consent of any person is not required, where there is a risk to a child victim survivor, including when there is also a risk to an adult victim survivor. As per an adult victim survivor, consent is also not required from any person where an ISE reasonably believes that sharing information is necessary to lessen or prevent a **serious threat** to an individual's life, health, safety or welfare.

Considerations when sharing information of a child victim survivor

As a principle, an ISE should give a child the opportunity to contribute to decisions that affect them. This includes seeking the views of a child victim survivor prior to sharing their information under Part 5A, where it is safe, appropriate, and reasonable to do so. When sharing information to assess or manage risk to a child, ISEs should:

- promote the agency of the child and other family members at risk of family violence by ensuring their views are taken into account (having regard to the appropriateness of doing so and the child's age and maturity) (section 144J (3)(a) FVPA)
- take all reasonable steps to ensure the information is shared in a way that:
  - plans for the safety of all family members at risk of family violence, and
  - recognises the desirability of preserving and promoting positive relationships between those family members and the child (section 144J (3)(b) FVPA).

ISEs should also take into consideration the age and stage of the child, and their cultural, sexual and gender identity.

Enabling a child to share their views and be involved in decision making can often increase their safety as it assists with the assessment of risk.

ISEs should consider which service/practitioner is best placed to seek the views of the child. This consideration should be based on expertise and existing relationships of trust with the child.

ISEs should also assess the extent of the perpetrator's use of power and coercive control over the family which may lead children to have divided loyalties to the perpetrator and the parent who is a victim survivor. Children may be scared and not want their information to be shared in case it would get the perpetrator in trouble, or, if they are fearful of the perpetrator, they may be concerned about heightening the risk to themselves or other family members.

If a child does not have capacity to share their views, in appropriate circumstances, an ISE should consider seeking the views of a parent (who is not a perpetrator) prior to sharing a child's information in order to maintain transparent and open communication.

Sharing a child's information without consent

In some situations it may be appropriate to share information without seeking the views of the child victim survivor or their parent (who is not a perpetrator), including when:

- the ISE reasonably believes that sharing confidential information is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare
- it is unreasonable, impractical or unsafe to seek the views of the child or parent
- the parent is underestimating the risk to the child
- it would otherwise not be in the best interests of the child to seek their views.

Sharing information when an adolescent is a victim survivor of family violence

ISEs should be mindful that adolescents may have strong views on when and how their information should be shared.

Where safe, appropriate and reasonable, ISEs should promote the agency of the adolescent who is at risk of being subject to family violence by seeking their views on when and how their information should be shared.

An ISE should determine the appropriateness of seeking and following the views of the adolescent. The ISE should consider the adolescent's:

- age and maturity
- understanding of the facts involved
- comprehension of the main choices
- ability to weigh up the consequences of the choices
- understanding of how the consequences affect them
- capacity to communicate their decision.

Note that children and adolescents who do not speak English as a first language, are from diverse communities or have a disability may need additional support and encouragement to express their views (See Chapter 8).

In some circumstances, the level of risk will be such that an ISE believes that information should be shared despite the adolescent's view that the information not be shared. If this is to occur, the ISE should explain to the adolescent how they have taken the views of the adolescent into account, and the reasons they believe that the information must be shared to either assess or manage risk to the adolescent.

Chapter 5 — Sharing information to assess and/or manage risk to a child victim survivor contains further information.

Adolescents who use violence

Family violence committed by adolescents is a distinct form of family violence and requires a different response to family violence by adults. Many adolescents who use family violence have been subject to violence themselves, and have other linked risk factors.

Therapeutic and diversionary responses to adolescents committing family violence are recommended, as adolescent family violence has unique characteristics and requires different responses to other forms of family violence. A therapeutic approach is more likely to improve identification of individual risk factors, such as previous exposure to family violence, trauma, mental health, disability and other factors that have been linked to this form of family violence.

Sharing information when an adolescent is both a victim survivor of family violence and is also at risk of committing family violence

Where an adolescent is both at risk of being subjected to family violence and at risk of committing family violence, Part 5A permits information to be shared about that adolescent without consent. However, if an ISE is sharing information to assess and manage the risk of an adolescent being subjected to family violence, it should consider the matters outlined in Chapter 5 — Sharing information to assess and/or manage risk to a child victim survivor.

ISEs should share information in a way that does not stigmatise or further isolate the adolescent as this can increase the risk of further family violence and lead to adverse outcomes for that adolescent.

Sharing information when an adolescent is at risk of committing family violence

When an adolescent is at risk of committing family violence against a family member who is a child, Part 5A permits information to be shared about any relevant person without their consent.

Where an adolescent is at risk of committing family violence against a family member who is an adult (and no child is at risk of being subjected to family violence), consent must be obtained from an adult victim survivor or third party prior to sharing their information, unless there is a serious threat (see Chapter 4).

Part 5A authorises ISEs to share information in circumstances where an adolescent is engaging in, or is at risk of engaging in, sexually abusive behaviours against a family member, as a form of family violence. ISEs should carefully consider who the information is shared with and for what purpose, and share information in a way that minimises stigma against the adolescent.

Information should be shared in a way that supports the therapeutic needs of the adolescent and may involve informing the adolescent that their information has been shared. This should only be done where the ISE has expertise in working with young people who use violence, believes it is appropriate, safe and reasonable to do so and is confident that informing the adolescent will not increase the risk to the victim survivor.

Notification

All notification requirements in the PDP Act and the HR Act continue to apply to the collection of personal and health information for child victim survivors, whether collected directly or indirectly including that all reasonable steps should be taken to notify child victim survivors except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

Although Part 5A does not require consent for sharing information to assess or manage risk to a child victim survivor, the ISE should inform the child victim survivor or parent (who is not a perpetrator) if their information has been shared, as long as this does not place the child victim survivor or other family members at further risk.

For further information see Chapter 6 — Sharing information about adolescents who are at risk of committing family violence.

Sharing information about Aboriginal people

Guiding principles when sharing information about an Aboriginal person

In recognition of the particular concerns that may be held by Aboriginal people engaging in the family violence system, ISEs must use the principles set out in section 144J of the FVPA for guidance when sharing information about an Aboriginal person under Part 5A.

ISEs must collect, use or disclose the confidential information of a person who identifies as Aboriginal in a manner that promotes the right to self-determination, including in a family violence context, is culturally safe and considers the person's family and community connections.

To demonstrate its compliance with the principles including promoting self-determination, all ISEs must:

- ask (at point of intake) all of their clients, including children, regardless of appearance, whether they identify as Aboriginal
- determine whether Aboriginal clients (including children) would prefer to receive a service from an Aboriginal-specific service, seek their client's views on what services their information should be shared with and make relevant referrals
- recognise the discrimination experienced by Aboriginal people and the impact of unjust government policies and practices
- demonstrate respect and consideration for Aboriginal people and culture
- work collaboratively with Aboriginal organisations and agencies to support the client in a culturally respectful manner.

The safety and security of victim survivors of violence remains the number one priority.

These principles must also be employed by services sharing information about a perpetrator who identifies as Aboriginal.

When sharing information about an Aboriginal person

ISEs should ensure that they are operating in a culturally safe manner and that their workers receive cultural competency training.

It is recognised that in an Aboriginal context, contributing factors to family violence include intergenerational grief and trauma resulting from the ongoing impact of the history of colonisation, dispossession of land and culture, and the wrongful removal of children from their parents.

This may also mean that Aboriginal victim survivors are less willing to trust government agencies and service providers, particularly where children are involved. It is important that ISEs be attuned to this when collecting information or requesting consent to share information. ISEs should also be mindful that sharing an Aboriginal client's information without consent or appropriate communication could affect the client's trust in the ISE. ISEs should therefore ensure their collection notices are tailored to the particular needs of Aboriginal clients. The victim survivor's choices about information sharing must be respected as much as possible.

Refer to Chapter 7 — Sharing information about Aboriginal people for further information.

Communities that may require additional considerations

ISEs should be aware, and respectful, of the many factors that may impact a person's experience of family violence and affect their response to information sharing.

Groups not yet discussed, whose circumstances may require additional consideration when accessing services and providing consent, include people with disabilities, people from culturally and linguistically diverse backgrounds, older people, people from lesbian, gay, bisexual, trans and gender diverse and intersex communities and people from small communities such as regional, rural and remote communities where it may be more difficult to maintain a person's anonymity.

Experiences of discrimination, oppression and trauma may make victim survivors from some of these communities particularly fearful of, or unwilling to, give consent to share their information.

Language and other communication barriers may also be a significant impediment to engaging with victim survivors when explaining the complex issues of consent and privacy legislation.

When sharing information about people from diverse communities

The Victorian Equal Opportunity and Human Rights Commission's 2017 Guideline *Family violence services and accommodation Complying with the Equal Opportunity Act 2010* provides examples of some common barriers and experiences of people from these and other communities, and provides guidance on inclusive and non-discriminatory service delivery to all those accessing the family violence sector.

Section 144J of the Act specifically requires ISEs to have regard to, and be respectful of, the person's cultural, sexual and gender identity and religious faith, in recognition of the fact that these aspects of identity and experience may affect their response to information sharing.

When sharing information or seeking consent from victim survivors to share information ISEs should:

- identify and address their own unconscious bias
- ensure the client understands information provided, or that necessary supports are given to enable comprehension. For example: providing an interpreter or translator, providing both written and verbal information, offering that person an advocate, etc.
- enquire about the client's concerns around information sharing and address those concerns
- clearly explain the ISE's obligations, including who information may be shared with, and for what purpose
- explain how sensitive information will be protected
- not assume that victim survivors will be comfortable with having information shared with close family members
- provide appropriate support or referral to specialist services.

More detail can be found in the Guidelines about concerns specific to:

- People who are lesbian, gay, bisexual, trans and gender diverse or have an intersex variation
- People from culturally and linguistically diverse backgrounds
- People with disabilities
- Older people
- People from rural, regional and remote communities

Suggestions for how ISEs may respond to these concerns and ensure an inclusive service model are also provided, as well as referrals to specialist services who can provide expert guidance and support. See Chapter 8 — Additional considerations for particular communities.

Record keeping and information management

Record keeping requirements

When sharing information about **any individual** under the Scheme an ISE must record:

- who requested the information, what information was requested and the date the request was made
- what information was shared, who the information was shared with and the date the information was shared
- a family violence risk assessment and safety plan in respect of a victim survivor about whom the information relates (including if they are a child), and any other family members who are at risk of being subjected to family violence.

When sharing information about **adult victim survivors** and **third parties** ISEs must also record:

- if consent was provided, a record of consent whether written, verbal or implied
- if information is shared without their consent:
  - the reason why consent was not obtained (ie. there was a serious threat or the information was to assess or manage risk for a child victim survivor)
  - whether it sought and obtained the views of the person and, if not, the reason why
  - whether the individual was informed that their information was shared without their consent.

When sharing information about a **child victim survivor**, ISEs must also record:

- whether it sought and obtained the views of the child or their parent (who is not a perpetrator or alleged perpetrator), and if not, the reason why
- whether the child victim survivor or their parent (who is not a perpetrator or alleged perpetrator) was informed that the information was disclosed.

Where an ISE **declines a request** from another ISE to disclose information about any person, it must record the request and the reason why it was declined.

If a **complaint** is made about the performance of an ISE's functions under Part 5A, it must record:

- the date the complaint was made and received
- the nature of the complaint and relevant details
- any action that was taken to resolve the complaint and to prevent or lessen the risk of further similar complaints
- time taken to resolve the complaint
- if any further action was taken.

In Victoria records must be kept and disposed of in accordance with the retention and disposal authorities set by the Public Record Office Victoria. Current records authorities can be seen at the Public Record Office Victoria website <http://prov.vic.gov.au/>.

Access and correction under privacy laws

Under privacy laws, people have a right to access and correct their personal and health information held by an organisation. However:

- ISEs can refuse a perpetrator (or alleged perpetrator) access to their information, or to information about their child or another person they have authority to represent, if the ISE reasonably believes that giving access would increase risk to the victim survivor from family violence.
- Information held by the Central Information Point is exempt and cannot be accessed by any person.
- Organisations should ensure that in providing a person access to information

that there is no unreasonable impact on the privacy of other individuals. Care should therefore be taken to review files and redact any information that relates to another person, including the perpetrator.

If a person is refused access to their records, that person may apply for a review of that decision by the relevant privacy regulator or the Victorian Civil and Administrative Tribunal. See Chapter 10 — Record keeping and information management for more information.

Access to information under freedom of information law

Every person has the right to seek access to documents held by organisations to which the *Freedom of Information Act 1982* (Vic) (FOI Act) applies. However:

- Documents in the possession of the CIP are exempt.
- A document will not have to be disclosed if its disclosure would involve the unreasonable disclosure of information relating to the personal affairs of a person (including a deceased person). When deciding this, a Minister or relevant agency that is an ISE must take into account whether a disclosure of that information to a perpetrator or alleged perpetrator would increase the risk to a victim survivor's safety from family violence.
- In notifying a person of its decision under the FOI Act, the relevant agency (that is an ISE) or Minister is not required to confirm or deny the existence of any document if doing so would increase the risk to a victim survivor's safety from family violence.

Whether a disclosure of information is likely to increase the risk of harm depends on the specific circumstances of each FOI request. This might occur where disclosure of a document would be likely to identify a victim survivor as a source of information about a perpetrator. Agencies are encouraged to ensure that their relevant business areas responding to FOI requests are aware of the family violence risk exception and are trained to identify family violence risk.

If an FOI request is refused, an application may be made for a review of the decision to the Victorian Information Commissioner.

Further information about record keeping, access and correction can be found in Chapter 10 — Record keeping and information management.

Interaction with privacy and other laws

Sharing with non-prescribed entities

ISEs need to rely on existing privacy laws or any other existing authorisation under another law to share information with, or request information from, entities that are not also prescribed as ISEs. Authorisation to share information for a family violence risk assessment or protection purpose under Part 5A can only be done between entities prescribed as ISEs.

ISEs can continue to share information under other Victorian laws

ISEs that are also authorised to collect, use or disclose information under another law can continue to do so, including where it is already allowed under the PDP Act, the HR Act and the *Children, Youth and Families Act 2005* (Vic) (CYFA). If information could lawfully be shared without relying on Part 5A, the requirements of Part 5A will not have to be met before doing so.

Application of existing privacy obligations

Existing privacy obligations under the PDP Act, HR Act or the *Privacy Act 1988* (Cth) (Commonwealth Privacy Act) will continue to apply unless they have been displaced under Part 5A (see below). ISEs should ensure that they are familiar with these obligations, as applicable, which include how personal, health and sensitive information should be handled.

A range of resources on complying with privacy laws are available at:

- the Office of the Victorian Information Commissioner's website <http://www.ovic.vic.gov.au>
- the Health Complaints Commissioner's website <http://hcc.vic.gov.au>
- the Office of the Australian Information Commissioner's website <http://www.oaic.gov.au>.

Organisations should review and update their privacy policies and other organisational materials to ensure that they reflect any changes to their organisation's management of personal or health information resulting from the introduction of Part 5A, and have regard to the general and family violence specific modifications to privacy laws.

Changes to Victorian privacy obligations when sharing under Part 5A

Part 5A provides ISEs with exceptions to the PDP Act and HR Act to assist ISEs assess and manage family violence risk.

As a result of these exceptions, ISEs are not required to:

- collect personal or health information about a perpetrator or alleged perpetrator directly from that person
- notify a perpetrator or alleged perpetrator where information about them is collected from someone else
- obtain consent from a perpetrator or alleged perpetrator before collecting 'sensitive information' about that person

- obtain consent from any person before 'sensitive information' is collected about them in relation to a child victim survivor
- provide a perpetrator or an alleged perpetrator access to their own personal or health information if the ISE reasonably believes that giving the person access would increase the risk of family violence to a victim survivor.
- In addition, Victoria's privacy laws allow any organisation bound by the PDP Act or HR Act to use or disclose personal or health information without consent if they reasonably believe it is necessary to lessen or prevent a *serious threat* to an individual's life, health, safety or welfare. This means organisations may act proactively to manage serious threats as soon as they become apparent, including serious threats that arise in contexts other than family violence. Information can be shared under these laws with services that are not ISEs.

For further information on the interaction of the Scheme with Victoria's privacy laws see OVIC's website <https://ovic.vic.gov.au/resource/family-violence-information-sharing-scheme-frequently-asked-questions/>.

Interaction with other laws

Part 5A overrides certain provisions in numerous other Acts that could prevent an ISE from being able to share some information under Part 5A. See Table 4 in Chapter 11 for further detail.

Secrecy and confidentiality provisions in other laws will continue to apply unless expressly overridden for the purposes of Part 5A, or allowed under those provisions. Where information is restricted from being shared under another law, that information should only be shared in compliance with that law.

It is recommended that an ISE obtain legal advice should they be in any doubt as to whether the information they seek to share may be restricted by another provision.

Responding to subpoenas

If an organisation receives a subpoena to produce information about a victim survivor or a perpetrator, that organisation should seek legal advice on how to respond before producing any information.

Information management and data security

Organisations must comply with their existing obligations regarding information management and data security. Among other things, this means organisations must take reasonable steps to ensure that the personal information or health information that organisation collects, uses or discloses is kept accurate, complete and up-to-date and, in the case of health information, relevant to their functions or activities.

Organisations must continue to comply with any applicable requirements that already apply to that organisation in relation to protective data security and are responsible for the protection of confidential information. See Chapter 11 — Interaction with privacy and other laws for further information.

Offences, complaints and good faith defence

Offences

Offences may apply where information is shared in ways that are not permitted by Part 5A — i.e for unauthorised use or disclosure or intentional or reckless unauthorised use or disclosure. These offences do not apply to victim survivors who have been provided with information by ISEs.

Other offences that may apply include those in state laws restricting information sharing that continue to apply and any applicable Commonwealth offences.

Protection for individual workers

If an individual worker acts in good faith and with reasonable care when sharing information under Part 5A, they will not:

- be held liable for any criminal, civil or disciplinary action for providing the information
- have breached any code of professional ethics or to have departed from any accepted standards of professional conduct.

Accountability of organisations

Organisations may be held to account for any interference with privacy though existing mechanisms, including complaints made under state and Commonwealth privacy laws and action in the Victorian Civil and Administrative Tribunal. Organisations should ensure that they have policies in place to protect against unnecessary breaches of privacy.

Departments that contract services may choose to reconsider funding arrangements with ISEs that repeatedly do not act in good faith or with reasonable care. For further information see Chapter 12 — Offences, complaints and good faith defence.

Complaints

In the first instance, complaints about a breach of a person's privacy should be made directly to an organisation. All organisations should have procedures in place for dealing with complaints and should make these available. ISEs are required to keep records of complaints made.

When receiving a complaint, an organisation should assess the complaint against the applicable state or Commonwealth privacy laws.

Complaints under state privacy laws

Complaints should be made to:

- **OVIC** when personal information is being collected or used by Victorian Government ISEs and other non-government ISEs that provide services on behalf of the Victorian Government **or** when neither the HR Act or the Commonwealth Privacy Act are applicable
- **HCC** when the ISE collects or uses health information.

The OVIC or HCC can investigate the complaint, attempt to resolve the complaint through conciliation processes and issue compliance notices for serious or flagrant privacy breaches arising from disclosures made under Part 5A. Civil penalties may also be sought against organisations for serious breaches.

More information about complaints to the OVIC <http://www.ovic.vic.gov.au> or the HCC <https://hcc.vic.gov.au> can be found on their respective websites.

Complaints when Commonwealth privacy law applies

When the Commonwealth Privacy Act applies, ISEs are able to share lawfully in accordance with Part 5A but must otherwise continue to meet their obligations under the Commonwealth Privacy Act.

Complaints may be made to the OAIC. If the OAIC chooses to investigate a complaint and it is considered likely that an interference with privacy has occurred, the OAIC may refer the matter to conciliation. If conciliation is not appropriate or does not resolve the complaint, then the OAIC will consider enforcement action.

For further information about complaints to the OAIC, please refer to the Commissioner's website <http://www.oaic.gov.au>.