Australian Capital Territory

Domestic Violence Agencies (Information Sharing) Ministerial Protocol 2026 (No 1)

Notifiable instrument NI2026–499

made under the

Domestic Violence Agencies Act 1986, s16AV (Information sharing protocols—Minister)

---

1 Name of instrument

This instrument is the *Domestic Violence Agencies (Information Sharing) Ministerial Protocol 2026 (No 1)*.

2 Commencement

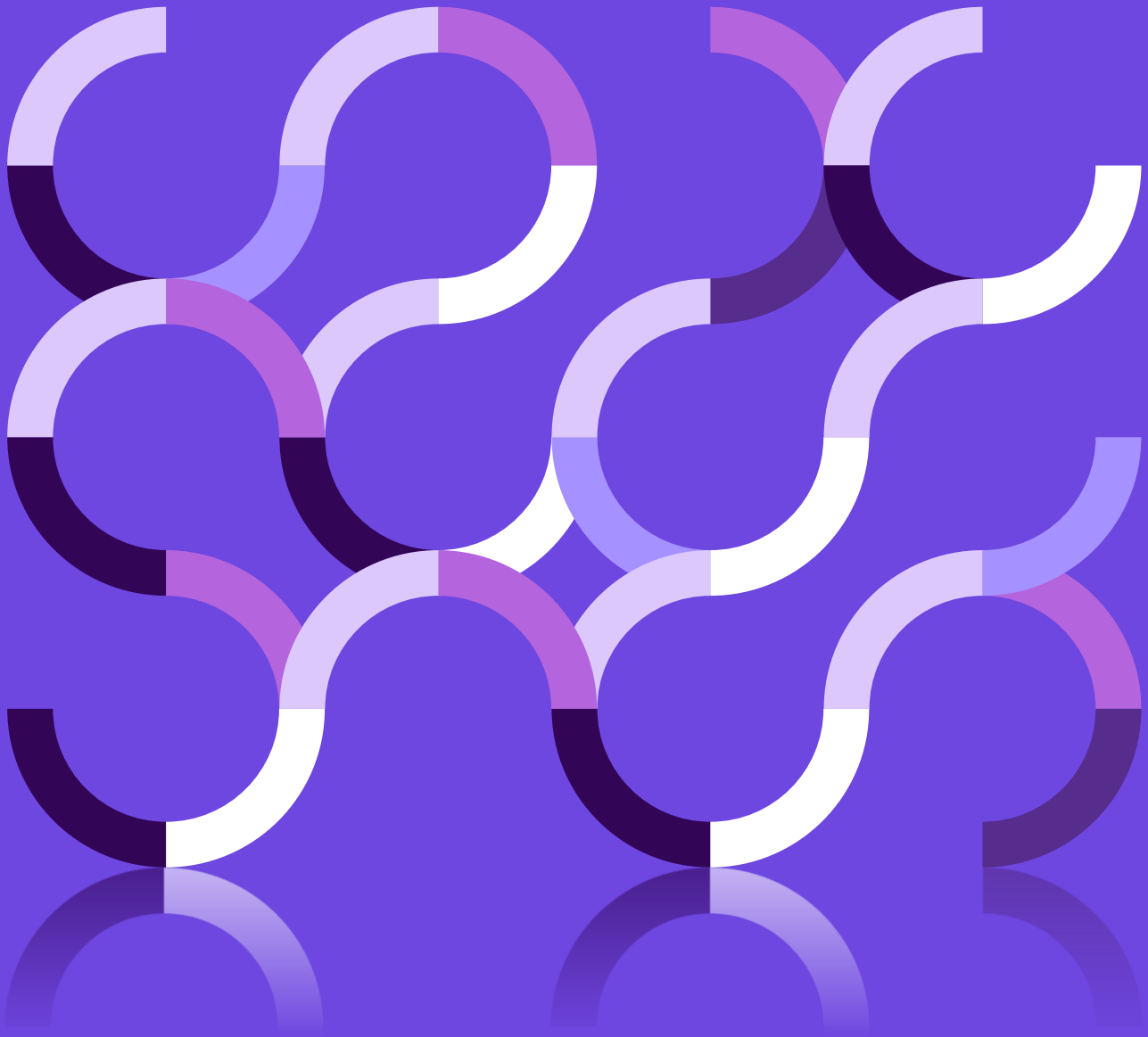
This instrument commences on 24 November 2026.

3 Approval

I make the Ministerial Protocol (Domestic and Family Violence Information Sharing) relating to the operation of Part 3 of the *Domestic Violence Agencies Act 1986* set out in Schedule 1.

Caitlin Tough MLA
Minister for the Prevention of Domestic, Family and Sexual Violence
4 November 2026

Schedule 1



Ministerial Protocol

Domestic and Family Violence Information Sharing Scheme

Protocols for sharing information under Part 3 of the *Domestic Violence Agencies Act 1986* for information sharing entities

Health and Community Services Directorate
October 2026

ACT Government

act.gov.au/DFV-info-sharing

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Acknowledgement of Country

We acknowledge the Ngunnawal people as traditional custodians of the lands of the ACT and region and recognise other people and families with connection to these lands. We acknowledge and respect their continuing culture and the contribution they make to the life of this city and this region. Responses to domestic and family violence are best led by the community, delivered by the community, for the community. We are committed to listening deeply and continuously while working together in partnership with the Aboriginal and Torres Strait Islander community, to strive to create an ACT community free from violence.

© Australian Capital Territory, Canberra 2026

Material in this publication may be reproduced provided due acknowledgement is made.

Produced by the Health and Community Services Directorate. Enquiries about this publication should be directed to the Health and Community Services Directorate.

GPO Box 158, Canberra City 2601

act.gov.au

Telephone: Access Canberra – 13 22 81

Publication: November 2026

Accessibility

The ACT Government is committed to making its information, services, events and venues accessible to as many people as possible.

If you are deaf, or have a hearing or speech impairment, and need the telephone typewriter (TTY) service, please phone 13 36 77 and ask for 13 22 81.

For speak and listen users, please phone 1300 555 727.

For more information on these services, contact us through the National Relay Service: www.accesshub.gov.au.

If English is not your first language and you require a translating and interpreting service, please telephone Access Canberra on 13 22 81.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

CONTENTS

1. INTRODUCTION 8
   - 1.1. Purpose of the Ministerial Protocol 10
   - 1.2. Purpose of the ACT Risk Assessment and Management Framework 10
   - 1.3. Principles for information sharing 11
   - 1.4. Terminology 11
2. HOW DOES INFORMATION SHARING UNDER PART 3 WORK? 15
   - 2.1. When can information be shared? 17
   - 2.2. Why can information be shared? 18
   - 2.3. What information can be shared? 21
   - 2.4. How should information be requested and shared? 22
   - 2.5. How can information be used? 25
   - 2.6. When you must not share information 31
3. WHO IS ALLOWED TO SHARE INFORMATION UNDER PART 3? 33
   - 3.1. Who is an ISE under Part 3? 34
   - 3.2. Who can ISEs share information with? 34
   - 3.3. Sharing with non-ISEs 34
4. THE INFORMATION SHARING COORDINATOR 35
   - 4.1. The role of the ISC 36
   - 4.2. When can the ISC require information sharing? 37
   - 4.3. How will ISEs interact with the ISC? 37
5. SHARING INFORMATION: PERSON OF CONCERN 39
   - 5.1. Consent is not required 40
   - 5.2. What information is relevant? 41
   - 5.3. Identifying the person of concern 43
   - 5.4. Sharing information with an at-risk person 45
6. SHARING INFORMATION: AT-RISK AND CONNECTED PEOPLE 47
   - 6.1. Consent is required 48
   - 6.2. Who should seek consent? 48
   - 6.3. When should you seek consent? 49
   - 6.4. Requirements for consent 51
   - 6.5. Sharing without consent 55
   - 6.6. Notification requirements 60
7. RECORD KEEPING 63
   - 7.1. Requirement to keep records 64
   - 7.2. What should be recorded? 64
   - 7.3. How should ISEs store information? 67
   - 7.4. How should information be destroyed? 68
   - 7.5. Accessing information 68
   - 7.6. Correcting information 69
   - 7.7. Special record obligations 69
8. GOOD PRACTICES IN INFORMATION SHARING 71
   - 8.1. Obtaining consent 72
   - 8.2. Reasonable supports 74
   - 8.3. Assessing capacity 75
   - 8.4. Working with priority cohorts 76
9. INTERACTION WITH OTHER LAWS 79
   - 9.1. DFVISS interaction with other laws 80
   - 9.2. Sharing information under other laws 81
   - 9.3. Subpoenas 83
10. OFFENCES, LIABILITY AND COMPLAINTS 85
   - 10.1. Offence for reckless disclosure or use 86
   - 10.2. Protection for workers 86
   - 10.3. Complaints 86

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

List of Tables

Table 1: Key definitions and concepts of the DFVISS 13

Table 2: Information sharing requirements - legislation and practice guidance 17

Table 3: Applying the thresholds for sharing information for a protection purpose .. 18

Table 4: Understanding when information can be shared for a secondary purpose under the DVA Act 29

Table 5: What the ISC must take into account when considering taking action for a protection purpose 36

Table 6: Requirements for communicating with the ISC 37

Table 7: Requirements for consent under the DVA Act 52

Table 8: Exceptions to sharing information without consent 55

Table 9: Practice guidance on how to practically apply the exception to consent 55

Table 10: Notification requirements under the DVA Act 60

Table 11: Matrix of what exceptions apply to each notification requirement 61

Table 12: Practice guidance for record keeping when sharing information 65

Table 13: Practice guidance for record keeping when refusing to share information 65

Table 14: Practice guidance for record keeping when taking an action under the DFVISS 66

Table 15: Practice guidance for record keeping when informing people about information use or disclosure 66

Table 16: Practice guidance for record keeping when an ISE receives a complaint 66

Table 17: Practice guidance on the elements of consent 73

List of Figures

Figure 1: Overview of the DFVISS 16

Figure 2: Flowchart - How to request information under the DFVISS 23

Figure 3: Flowchart - Responding to a request for information under the DFVISS 24

Figure 4: Seek consent when safe, reasonable and appropriate 49

Figure 5: Flowchart - Should I seek consent? 50

Figure 6: Flowchart - Sharing information about at-risk adults and connected people 53

Figure 7: Flowchart - Sharing information about at-risk children and young people 54

Figure 8: Flowchart - Sharing information without consent - At-risk person 56

Figure 9: Summary of the five record keeping checkpoints across the DFVISS 64

Figure 10: Five elements of consent 73

Figure 11: Flowchart - Can I share information? (Information sharing laws in the ACT) .. 82

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

EXECUTIVE SUMMARY

This is the first Ministerial Protocol making operational rules and providing best practice guidance on sharing information under Part 3 of the *Domestic Violence Agencies Act 1986*. This work was informed by the important contributions of information sharing entities and the specialist domestic and family violence sector in the ACT. We also acknowledge the work of other Australian jurisdictions, namely Victoria's Family Violence Information Sharing Guidelines and the Northern Territory's Domestic and Family Violence Information Sharing Guidelines, which have informed the ACT's Ministerial Protocol.

Effective responses to domestic and family violence, which place victim-survivors at the centre, rely on collaboration, coordination and integration across the service system. Information sharing to assess and manage risk is a vital element of coordination to ensure services can obtain the 'full picture' of a person's risk of domestic and family violence.

In recent years, several ACT-based reports have identified the need for information sharing law reform in the domestic and family violence context. In particular, Glanfield's Report of the *Inquiry: Review into the system level responses to family violence in the ACT*, the findings and recommendations from the *Review of Domestic and Family Violence Deaths in the ACT*, the *Review of the Implementation of the Family Violence Act 2016* and the *ACT Domestic Violence Service System Final Gap Analysis Report* each highlight significant barriers to information sharing. This includes a lack of clarity about when and how agencies can share information, and institutional cultures which emphasise privacy and secrecy protections, particularly in relation to sharing information about people using violence.

Part 3 of the *Domestic Violence Agencies Act 1986* establishes the ACT Domestic and Family Violence Information Sharing Scheme (DFVISS). The DFVISS is supported by the legislation, Ministerial Protocol and ACT DFV Risk Assessment and Management Framework.

The DFVISS aims to support a cultural shift in information sharing practice through changing the authorising environment. Providing a clear legal framework for information sharing entities to deal with information for a protection purpose will break down existing practice barriers to information sharing, collaboration and integration. This new framework clearly authorises the sharing of information about people using violence without their knowledge or consent.

There are 4 purposes for broadening the authorising information sharing environment:

- to prevent and reduce domestic and family violence;
- to promote the safety, protection and wellbeing of victim-survivors;
- to hold people who use violence to account; and
- to promote the development of skills and expertise of government and community-based organisations.

Through enabling the timely sharing of relevant information, the DFVISS will support information sharing entities to keep people who use violence in view, and promote the safety of victim-survivors.

The ACT DFV Risk Assessment and Management Framework is a key building block of the DFVISS. It outlines best practice evidence to enable practitioners, of varying skills and knowledge, to better assess and manage domestic and family violence risk in a consistent and unified way.

By using Part 3, the guidance of this Ministerial Protocol, and the risk evidence of the ACT DFV Risk Assessment and Management Framework, information sharing entities will be better placed to provide safer responses to domestic and family violence in the ACT.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

OVERVIEW OF THE DFV INFORMATION SHARING SCHEME

Preventing domestic and family violence is everyone's responsibility

- Domestic and family violence (DFV) causes serious harm to victim- survivors and the ACT community.
- In recent years, several ACT reports and reviews identified the need for reform to information sharing laws, to address institutional cultures which emphasise privacy and secrecy protections.
- Sharing information across services is one important way we can better work together to hold people who use violence to account and support the safety of victim-survivors.
- When different agencies have different information about a DFV matter, this information in isolation may not show that a person is at risk of harm.

Mandatory reporting, reportable conduct and other information sharing laws still apply

- Information sharing under Part 3 of the *Domestic Violence Agencies Act 1986* does not replace existing information sharing and mandatory reporting laws.
- Under these laws, there are situations where information may be shared, reported or disclosed, even where consent has not been given.
- For example, information may be disclosed under the *Information Privacy Act 2014* if an organisation reasonably believes it is necessary to lessen or prevent a serious threat to a person's life, health or safety.
- The DFV Information Sharing Scheme creates a new authorising law, in addition to these existing laws and obligations.

What information can you share under the DFVISS?

- Relevant information in any form, whether true or not (including opinion or advice) can be shared under the DFVISS. This includes personal and health information.
- The main guiding principle is that the information must be necessary to assess or manage domestic and family violence risk (known as a 'protection purpose').
- The intent of the DFVISS is to authorise ISEs to share information to build a picture of risk, including when the level of risk is unknown or when there is no known imminent threat.

DFV information sharing laws apply to 'information sharing entities'

- Under Part 3 of the *Domestic Violence Agencies Act 1986*, prescribed 'information sharing entities' (ISEs) can be required to share information. This includes certain government agencies and non-government schools.
- This will help organisations assess and respond to DFV risk in an integrated way.
- Over time, more agencies, including non-government organisations, can become part of the Information Sharing Scheme.

Can you share information about a person using violence without their consent?

- Yes. ISEs must not tell a person using violence that they have shared their information, and ISEs must not seek the person's consent to share their information. This is a critical part of the Information Sharing Scheme.
- This includes sharing personal or health information, as long as sharing the information is for a protection purpose.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Can you share information about a victim-survivor without consent?

- No. An ISE generally needs the consent of a victim-survivor before sharing information about them. This is a key part of supporting victim-survivor agency, and ensuring that system responses do not create additional risk.
- However, some exceptions apply where it is not safe or possible to seek consent, or where there may be a serious risk if you do not share their information.
- The safety of a person experiencing DFV is always paramount in deciding if information can be shared without their consent.

When can information be shared?

- ISEs can only share information if it is for a protection purpose, and the other DFVISS requirements have been met. In limited circumstances, information may also be shared for a 'secondary purpose'.
- Part 3 allows ISEs to proactively share information with other ISEs and the victim-survivor.
- If an ISE has received a request and the DFVISS thresholds are met, the ISE is required to share relevant information.
- Where an ISE has not complied with a request to share information from another ISE, the Information Sharing Coordinator can require the ISE to disclose the requested information, if the information sharing is not prohibited.

When is it prohibited to share information?

- ISEs are not allowed to share information if a 'relevant ground' under the *Domestic Violence Agencies Act 1986* applies.
- This recognises there are limited situations where sharing information under Part 3 cannot occur due to other policy reasons, including when sharing information could: endanger a person's life or safety; prejudice a court case or investigation; or breach an order of a court or tribunal.
- ISEs are also not allowed to share information that is specifically restricted or protected under other laws.

What do ISEs need to do?

- ISEs must comply with any requirements of this Ministerial Protocol. These requirements are stated throughout.
- ISEs should review and align their policies and procedures with obligations under the DFVISS.
- ISEs must ensure their policies, practices and procedures for sharing information align with the ACT DFV Risk Assessment and Management Framework.
- ISEs need to be aware of their record keeping obligations in this Ministerial Protocol.
- All ISEs should respond to requests to share information in a timely manner.
- Where a request is urgent or a serious risk has been identified, ISEs must respond without unreasonable delay.
- There will be times where ISEs will need to communicate with the Information Sharing Coordinator. ISEs must familiarise themselves with these obligations under the Scheme.

What if you are not an ISE?

- If you are not an ISE, you may still be able to share information about a person (including a person of concern) without their consent.
- Other mandatory reporting and information privacy laws may also require or allow information sharing in certain situations.
- All organisations (even if they are not an ISE) should have policies and procedures in place so they can identify and respond to DFV, including to meet any mandatory reporting and information sharing obligations under other laws.

Where can I get more information?

- Information and resources are available at the dedicated DFV Information Sharing Webpage at www.act.gov.au/DFV-info-sharing.
- The ACT Domestic and Family Violence Risk Assessment and Management Framework is a key part of the DFVISS. You can access it at www.act.gov.au/DFVrisk.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

1. INTRODUCTION

Timely and appropriate information sharing can prevent serious harm and save lives. This Chapter describes the role of this Ministerial Protocol, the ACT Domestic and Family Violence Risk Assessment and Management Framework, and the guiding principles and concepts underpinning information sharing under the Domestic and Family Violence Information Sharing Scheme (DFVISS).

Many different services and practitioners – such as police, specialist domestic and family violence services, justice agencies, child protection and health services – can become involved in a case. Effective, coordinated responses require agencies and services to work together and may depend on sharing relevant information.

Information sharing is important in assessing and managing risk, as each service may hold different information about the circumstances and risks in each case.

ⓘ Remember

The Ministerial Protocol is not legal advice. Organisations that are prescribed 'information sharing entities' should seek their own independent legal advice, if required.

Key Points

- Part 3 of the *Domestic Violence Agencies Act 1986* (DVA Act) creates the DFVISS.
- The safety principle is enshrined under the DVA Act and applies to all information sharing that occurs under Part 3. This principle requires ISEs to prioritise the safety and protection of people experiencing DFV, as far as possible.
- ISEs are required by law to comply with any information sharing requirements of the Ministerial Protocol and the ACT Domestic and Family Violence Risk Assessment and Management Framework.
- The Ministerial Protocol does not replace an organisation's own policies, procedures and systems in relation to information sharing.
- All ISEs can use the Ministerial Protocol to adapt their policies, procedures and systems to reflect DFVISS requirements.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

1.1. Purpose of the Ministerial Protocol

The Ministerial Protocol is law under the DVA Act. ISEs **must** comply with any requirements of this Ministerial Protocol when sharing information under Part 3.

The Ministerial Protocol has been developed to support Information Sharing Entities (ISEs) to share information to assess and manage DFV risk. It states requirements for dealing with information under Part 3, as well as outlining best practice guidance to support ISEs to meet their obligations in a safe and coordinated way. The key below describes how ISEs can navigate the requirements, guidance and case studies throughout the Protocol.

Protocol Requirements

Specific obligations included in the Ministerial Protocol, in addition to the DVA Act.

Practice Guidance

Best practice and operational guidance to help ISEs meet their obligations under the DFVISS and engage in safe information sharing practice.

Case Studies

A practical scenario of DFV information sharing across different information sharing scenarios and topics.

DVA Act Requirements

Summarised requirements that are made by Part 3 of the DVA Act, which created the DFVISS.

1.2. Purpose of the ACT Risk Assessment and Management Framework

The ACT Domestic and Family Violence Risk Assessment and Management Framework (ACT RAMF) is a key building block of the DFVISS. Like the Ministerial Protocol, it is law under the DVA Act and ISEs must comply with any requirements of the ACT RAMF when sharing information under Part 3.

Why the ACT RAMF?

The ACT RAMF outlines a shared understanding of the nature and dynamics of domestic and family violence. The ACT RAMF relies on best practice evidence to enable practitioners, of varying skills and knowledge, to assess and manage domestic and family violence risk in a consistent and unified way.

Information sharing under the DFVISS will require ISEs to understand, identify and respond to DFV in a safe, evidence-based and coordinated way. The ACT RAMF provides the necessary tools and guidance for ISEs to screen, assess and respond to identified DFV risks. In practice, this will help ISEs to know they are appropriately sharing information relevant to DFV risk, including how to triage matters based on identified risks.

The **roles and responsibilities** of agencies, services and practitioners are organised by 'tiers'. These tiers are based on knowledge and skills. Depending on what tier level an agency, service or practitioner is, they will use different elements of the ACT RAMF relative to their skills, knowledge and expertise.

Practice Guidance

- Information sharing entities should review the ACT RAMF to understand their specific roles and responsibilities when supporting responses to domestic and family violence.
- Throughout this Ministerial Protocol, specific requirements are stated about how ISEs must apply the ACT RAMF in specific information sharing contexts.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

1.3. Principles for information sharing

The DVA Act identifies the safety principle, which applies to information sharing under the DFVISS. This principle requires **ISEs to prioritise, as far as possible, the safety and protection of a victim-survivor.**

ISEs should also be guided by the following overarching principles when sharing information:

- **Proportionality** – ISEs should only share relevant information to the extent that is necessary to assess and manage domestic and family violence risk (that is, achieve a protection purpose).
- **Collaboration** – ISEs should coordinate services for the purpose of risk assessment and management, in a way that respects the functions and expertise of each entity.
- **Agency** – ISEs should promote the autonomy and agency of victim-survivors by partnering with them, seeking their views and keeping them informed about how their information will be used. Victim-survivors must be afforded the right to exercise autonomy and control over the decisions and choices in their lives.
- **Responsibility** – ISEs should take responsibility to identify and respond to DFV and take action within their roles and responsibilities as informed by the ACT RAMF.
- **Accountability** – ISEs should share information to ensure that people who use violence are held to account, and their behaviours and impacts are held in view when sharing information. See the ACT RAMF for guidance on ensuring the full responsibility for the violence is held with the person of concern.
- **Centring children and young people** – Children and young people must be recognised as victim-survivors in their own right, either because of their experiences of DFV among others in the home or because of child maltreatment. Children experience fear and trauma even if they have not been physically harmed.

1.4. Terminology

The definition of domestic and family violence for the DFVISS is the definition set out in *Family Violence Act 2016*. The below definition additionally emphasises the pattern-based nature of DFV, as reflected in the ACT RAMF and in broader policy and operational settings.

Domestic and family violence broadly describes any behaviour or pattern of behaviours aimed at controlling or intimidating a former or current partner or family member. Behaviours are highly contextual, and can include behaviour that is physically, sexually, emotionally, psychologically, spiritually or culturally abusive. This definition of DFV underpins the shared understanding of DFV in the ACT RAMF.

What is central to our understanding of DFV in both policy and legal settings, is that it is a pattern of behaviours designed to control or intimidate a victim-survivor, rather than as an incident or series of incidents of violence. It is this underlying pattern of power and control by one person over another, often described as coercive control, that differentiates DFV from other forms of violence.

The term **domestic violence** usually refers to violence against an intimate partner or ex-partner, while **family violence** may include violence perpetrated against children, older people, of parents by children, and other kin or family members. Many Aboriginal and Torres Strait Islander communities prefer the term family violence to reflect broader family and kin relationships.

This document uses the terms **victim-survivor** and **person using violence**. We acknowledge that some victim-survivors, ISEs or professionals may identify with or use different terms, as language depends on context and the distinct experience of people impacted by violence and those working alongside them.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Table 1 summarises key words and concepts in the DFVISS. Please refer to the definitions under the DVA Act as the primary source of information.

TERM	DESCRIPTION
DOMESTIC AND FAMILY VIOLENCE (DFV)	Refer to the definition of 'family violence' in the *Family Violence Act 2016*. Please also see the shared understanding of domestic and family violence in the ACT RAMF.
DVA ACT	The DVA Act refers to the *Domestic Violence Agencies Act 1986*, which creates the DFV Information Sharing Scheme (DFVISS) in the ACT.
DFV INFORMATION SHARING SCHEME (DFVISS)	DFVISS refers to the dedicated legal framework for sharing information to assess, prevent and manage DFV risk in the ACT. The DFVISS includes: • Part 3 of the *Domestic Violence Agencies Act 1986*; • The Ministerial Protocol (and any entity protocols); and • The ACT Domestic and Family Violence Risk Assessment and Management Framework.
MINISTERIAL PROTOCOL	The Ministerial Protocol is a required part of the DFVISS, made under Part 3 of the DVA Act, to support its practical operation. The Ministerial Protocol can make requirements for dealing with information under the DFVISS, as well as including information to provide guidance to information sharing entities (ISEs) on how to comply with information sharing requirements.
ENTITY PROTOCOL	Information sharing entities may make protocols about dealing with information under the DFVISS. An entity protocol must be consistent with the ACT RAMF and the Ministerial Protocol. Please refer to Part 3 of the DVA Act for other requirements about entity protocols.
ACT DOMESTIC AND FAMILY VIOLENCE RISK ASSESSMENT AND MANAGEMENT FRAMEWORK (ACT RAMF)	The ACT RAMF is a required part of the DFVISS, made under Part 3 of the DVA Act, to support the operation of the DFVISS. The ACT RAMF is an ACT specific framework that provides practical guidance and tools to help identify, assess and manage DFV risk in a consistent and coordinated way. The ACT RAMF and other supporting documents can be accessed online.
INFORMATION SHARING ENTITY (ISE)	ISEs are the entities, organisations or agencies that are allowed to deal with information under Part 3 of the DVA Act. The DVA Act specifies who is included as an ISE. The Minister may also declare an entity to be an ISE (what is known as a 'restricted entity').
RESTRICTED ENTITY	A restricted entity means a declared information sharing entity with certain (or all) protection purposes stated in the declaration.
DEAL WITH INFORMATION	'Deal' with information means collecting, using or disclosing information.
INFORMATION	Means information in any form, whether it is true or not, and includes an opinion and advice.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

TERM	DESCRIPTION
SENSITIVE INFORMATION	Means information or an opinion about an identified individual, or an individual who can be reasonably identified. Like the definition of 'information', sensitive information can be true or not and includes opinion, whether in material form or not.
PROTECTION PURPOSE	A 'protection purpose' includes a broad range of activities for establishing, assessing, managing, preventing and reducing risks of domestic and family violence. ISEs are allowed to 'deal with information' when it is for a protection purpose.
AT-RISK PERSON (VICTIM-SURVIVOR)	An at-risk person is someone who has experienced, is experiencing, or may experience DFV. An at-risk person includes children and young people, recognising them as victim-survivors. Any reference to a 'victim' or 'victim-survivor' in this Ministerial Protocol is taken to refer to an 'at-risk person' under the DFVISS.
PERSON OF CONCERN (PERSON USING VIOLENCE)	A person of concern is a person who has engaged in, is engaging in, or is at risk of engaging in DFV. This could be an adult, child or young person. Any reference to a 'person using violence' or 'perpetrator' in this Ministerial Protocol is taken to refer to 'person of concern' under the DFVISS.
CONNECTED PERSON (THIRD PARTY)	A connected person is someone who has information that is relevant to a protection purpose, or information about the connected person is relevant to a protection purpose. A connected person could include family members (including children and young people), friends or other people connected to an at-risk person or person of concern. This is a third party other than an at-risk person or person of concern.
INFORMATION SHARING COORDINATOR (ISC)	The ISC is a specific role created by Part 3 of the DVA Act. It is responsible for facilitating information sharing under the DFVISS, provides independent oversight over the operation of the DFVISS, and has the power to compel information sharing in certain situations.

Table 1: Key definitions and concepts of the DFVISS

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2. HOW DOES INFORMATION SHARING UNDER PART 3 WORK?

Chapter 2 gives a broad overview of Part 3 of the DVA Act, and how the DFVISS works to enable information sharing. The DFVISS creates a new authorising environment to promote and support coordination and collaboration between information sharing entities to establish, assess, prevent, reduce and manage domestic and family violence risk.

ⓘ Remember

- The intent of the DFVISS is to share information to build a bigger picture of risk, including when the level of risk is unknown or there is no imminent or serious threat.
- Information sharing is essential to risk assessment and management of DFV. The relevance of information is not always clear when seen in isolation of other information, and ISEs will therefore often need to share information to understand what is relevant.

Key Points

- If an ISE has received a request under the DFVISS, the ISE is generally **required** to share information with the requesting ISE. ISEs can also **proactively** share information with other ISEs and the at-risk person (see Chapter 2.1).
- The DFVISS authorises information sharing between ISEs, when necessary to establish, assess, prevent, reduce and manage DFV risk – any of these purposes are a **protection purpose**. See Chapter 2.2 for additional information sharing requirements.
- Information sharing practices need to hold the person using violence in view. This is because a protection purpose fundamentally relates to assessing and managing risk of DFV. This purpose can be best achieved by focusing on the behaviours, actions and circumstances of the person of concern.
- There are a limited number of scenarios where information can be shared or used for a different purpose, other than a protection purpose (a **secondary purpose**). This includes sharing information to meet other legal obligations (e.g. mandatory reporting) or sharing under another law for other urgent or serious circumstances (see Chapter 2.5).
- ISEs can share information about a **person of concern** without their consent or knowledge. This is a key part of the DFVISS (see Chapter 5).
- When sharing information about an **at-risk or connected person**, their consent is always required unless an exception applies (see Chapter 6).
- Where an ISE has not complied with a request to share information from another ISE, the **Information Sharing Coordinator** can require the ISE to share information (see Chapter 4).
- There are a limited number of situations where ISEs are not allowed to share information under the DFVISS (see Chapter 2.6).
- Figure 1 provides a one-page overview of the DFVISS, including who is in the DFVISS, the purposes for information sharing, when information can and cannot be shared, consent requirements and necessary steps to take after information has been shared.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Overview of the DFV Information Sharing Scheme (DFVISS)

Figure 1 provides a one-page overview of the core components of the DFVISS.

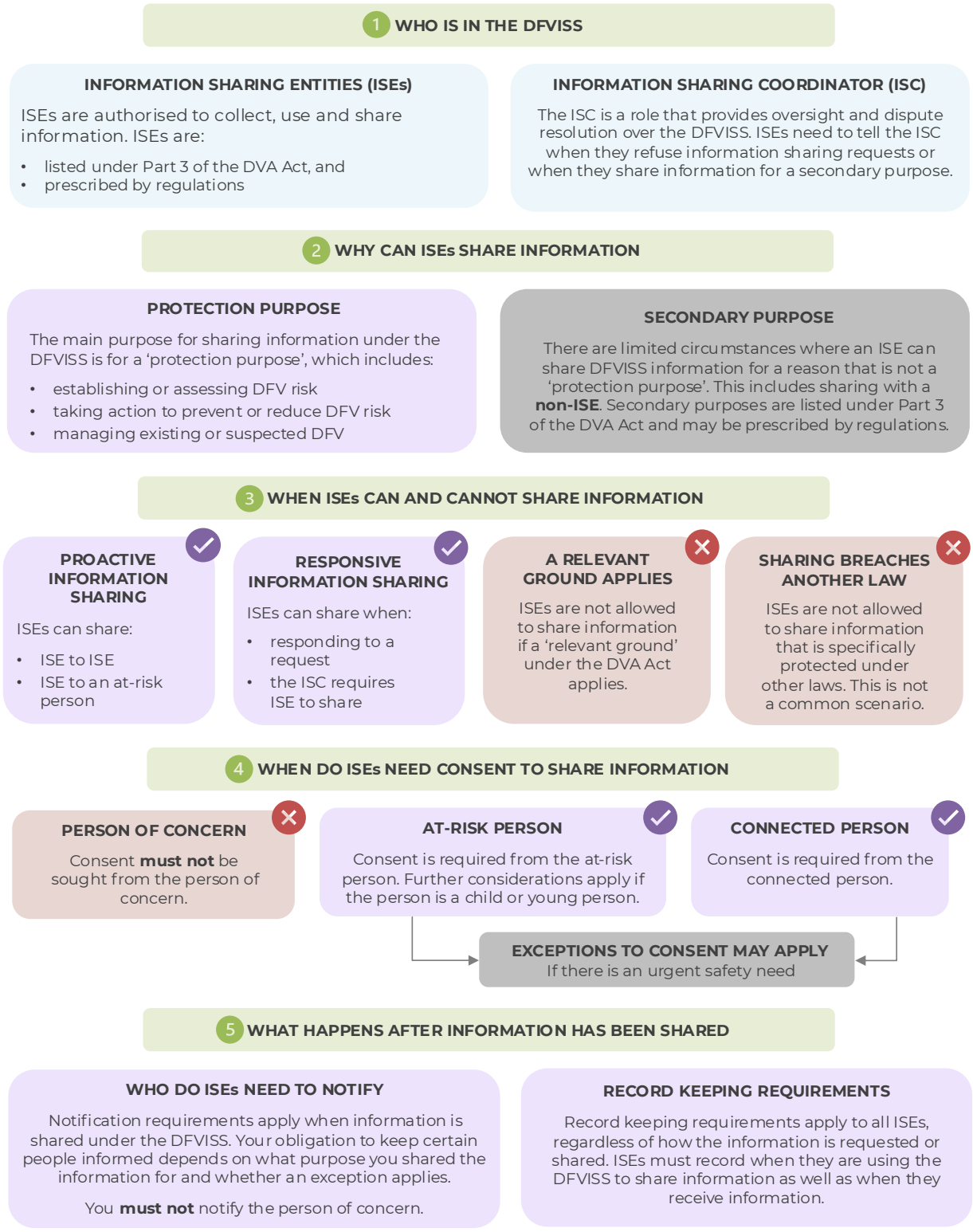


Figure 1: Overview of the DFVISS

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2.1. When can information be shared?

Part 3 of the DVA Act creates requirements that ISEs need to comply with when sharing information. Division 3.2 of the DVA Act sets out the main information sharing requirements, and Division 3.3 describes when ISEs can and must share information.

Provided the requirements have been met, and there is no reason that information sharing is prohibited (in Chapter 2.6):

- an ISE may share information with another ISE on its own initiative (**proactive**)
- an ISE may share information with an at-risk person on its own initiative (**proactive**)
- an ISE must share information when it has been validly requested by another ISE (**mandatory**)
- if an ISE has not complied with a request to share information from another ISE, the ISC can require an ISE to disclose the requested information (**mandatory**)

When sharing information with other ISEs, the information needs to be **relevant to the other ISEs functions**.

Table 2 details a summary of the main DVA Act information sharing requirements, together with practice guidance to support implementation.

Requirement	What is required	Practice Guidance
Purpose requirement Section 15	An ISE must only deal with information if it is necessary for: • a protection purpose; or • a secondary purpose.	• **Protection purpose** (see Ch 2.2, 2.5) • **Secondary purpose** (see Ch 2.5) – if sharing for a secondary purpose, an ISE needs to only comply with the secondary purpose requirements in Part 3 of the DVA Act.
Consent requirements Section 16(1)(a)	An ISE must comply with any requirements under the DFVISS for consent (including exceptions to consent).	• **Person of concern** – consent not required under any circumstance (see Ch 5). • **At-risk or connected person** – consent generally required unless an exception applies (see Ch 6).
Operational requirements Section 16(1)(b)	An ISE must comply with any requirements under the • ACT RAMF • Ministerial Protocol • An entity protocol (if there is one).	• **Ministerial Protocol Requirements** – requirements stated throughout this document. • **ACT RAMF** – the Ministerial Protocol describes how the ACT RAMF must be used to support evidence-based risk assessment and management practice under the DFVISS.
Restricted entity requirements Section 16(1)(c)-(d)	Information can only be disclosed and used for the protection purposes stated in the restricted entity's declaration.	• **Restricted entity** – this only applies if an ISE is sharing information with a restricted entity, or a restricted entity proposes to use information it has received (see Ch 2.5 and 3.2).
Personal factor requirements Section 16(2)	When exercising a function under the DFVISS in relation to an at-risk person, the ISE must consider specific personal factors prescribed by legislation for certain cohorts.	• **Personal factors** – for best practice guidance to support ISEs to meet this requirement, see Ch 8.4.

Table 2: Information sharing requirements - legislation and practice guidance

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2.2. Why can information be shared?

Key Points

- The main purpose for sharing information under the DFVISS is for a **protection purpose**. Certain thresholds need to be met when sharing information for this purpose.
- Information sharing practices need to hold the person using violence in view. This is because a **protection purpose fundamentally relates to assessing and managing risk of DFV**. This purpose can be best achieved by focusing on the behaviours, actions and circumstances of the person of concern.
- Information obtained under the DFVISS can also be shared or used other than for a protection purpose in limited situations (a **secondary purpose**). Different considerations apply (see Chapter 2.5).

Information sharing thresholds – Protection purpose

The DFVISS allows both **proactive** and **mandatory** information sharing, when certain thresholds are met. These are set out under Part 3 of the DVA Act, and are summarised as follows:

- The ISE believes DFV has occurred, is occurring, or is at risk of occurring;
- The ISE believes the disclosure is necessary for a protection purpose; and
- The ISE believes sharing the information is relevant to the functions of the other ISE (this applies *only* when sharing between ISEs).

Applying the thresholds in practice

Table 3 summarises the thresholds and practice guidance when sharing information for a protection purpose.

Threshold	Practice Guidance
DFV has occurred, is occurring, or is at risk of occurring	• **Reasonable belief** is required (see Ch 2.2) • **Protection purpose (establish and assess)** (see Ch 2.2, 2.5) – ISEs will sometimes need to share information to *ascertain* if someone is experiencing or engaging in DFV. • **Identification and misidentification** (see Ch 5.3) – ISEs may sometimes need to correctly identify the person that is most in need of protection (i.e. the at-risk person or primary victim), by relying on the guidance in this Ministerial Protocol and the ACT RAMF. This will help ISEs apply other DFVISS obligations about consent.
Necessary for a protection purpose	• **Reasonable belief** is required (see Ch 2.2) • **Necessary for a protection purpose** (see Ch 2.2 and 2.5) – Establish and assess risk (see Ch 2.5) – Prevent, reduce and manage risk (see Ch 2.5) • **Sharing information with an at-risk person** – An ISE can share information directly with an at-risk person, if it is necessary for a protection purpose (see Ch 5.4)
Sharing the information is relevant to the functions of the other ISE	• **Reasonable belief** is required (see Ch 2.2) • **Relevant to ISE functions** (see Ch 2.2) – different ISEs will have different functions and roles in the broader service system (e.g. supporting victim-survivor safety, therapeutic supports, investigative functions, perpetrator accountability). • **Restricted entity** (see Ch 3.1) – ISEs should ensure they only share information for the specific protection purposes listed in the restricted entity's declaration

Table 3: Applying the thresholds for sharing information for a protection purpose

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Protocol Requirement

ISEs **must** (where relevant) rely on the **ACT RAMF** when:

- Identifying whether DFV has occurred, is occurring or is at risk of occurring; and
- Identifying what information may be relevant to a protection purpose.

Necessary for a protection purpose

Generally, an ISE must only perform a function under Part 3 of the DVA Act if it is for a protection purpose. A protection purpose means any of the following:

- **establish or assess** if someone is experiencing or at risk of experiencing DFV
- **establish or assess** if someone is engaging in, or is likely to engage in DFV
- **prevent or reduce** the risk of DFV occurring
- **manage** DFV, or manage suspected DFV

Whether something is necessary for a protection purpose will depend on the situation. ISEs may consider:

- How is the information relevant to one or more protection purposes?
- Is the intention of sharing the information to increase visibility of the person using violence?
- When sharing the information, am I placing responsibility for the violence with the person using violence?
- Can the information be used to support protective activities in line with risk assessment and risk management practices?

Practice Guidance

- A protection purpose is a specific, but broad concept designed to capture activities that support evidence-based risk assessment and management practices. This includes authorising information sharing to build a picture of risk, including when the level of risk is unknown or there is no imminent threat.
- Whether sharing information is *necessary* for a protection purpose will depend on whether the information is relevant to, or supports, risk assessment and management practices.
- Risk assessment and management practice should always place full responsibility for the violence with the person of concern, as described in the ACT RAMF.
- This approach needs to be reflected in information sharing practices, by sharing information that focuses on assessing and managing the risk created by the perpetrator's behaviours, actions and circumstances.
- See Chapter 2.5 for more detailed practice guidance on dealing with information for a protection purpose.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Functions of the ISE

When sharing information with another ISE, the information needs to be relevant to their functions. This requirement ensures that information is being appropriately shared across the service system.

Practice Guidance

Whether information is relevant to an ISEs function(s) can be understood with reference to the tiers of responsibilities in the ACT RAMF. Some additional considerations about whether information is relevant to an ISEs functions include:

- Is the receiving ISE or requesting ISE in a position to **take action** to use the information to manage the risk?
- Is the information **required** for the ISE to take that action, or could the ISE take that action without the information?
- If sharing with a **restricted entity**, are you sharing information with them that aligns with the specific protection purpose relevant to that entity? (see Chapter 3.1).

Reasonable belief

Each threshold requires an ISE to hold a **reasonable belief**. A 'reasonable belief' is an honest belief that is well-founded, and it must be held on reasonable grounds. **A reasonable belief does not mean the ISE has to be certain, or that there is evidence proving particular facts**. However, a reasonable belief is more than a suspicion.

Practice Guidance

Whether a belief is reasonable should be determined with reference to the ACT RAMF. It may also depend on other circumstances, including:

- the information the practitioner already has;
- the practitioner's skills, training and experience (for example, a specialist DFV practitioner requesting information may have specific expertise in assessing DFV risk and requesting information from other agencies); or
- the urgency of the situation.

Case Study 1: What is a 'reasonable belief'

Cynthia and Ethan bring their 8-month-old child to a playgroup in the West Belconnen Child and Family Centre. Child and Family Centres (CFC) are ISEs under the Scheme. During the session, a CFC staff member notices that Cynthia has visible bruising on her arms and face. The staff member also observes the interactions between Ethan and Cynthia, noticing that Ethan becomes increasingly agitated towards Cynthia and calls her "stupid" when she accidentally drops her child's toy on the ground. Later, when Ethan is no longer present, the staff member checks in with Cynthia and asks if she is okay and whether she might be experiencing DFV. Cynthia does not answer directly but says that things have been hard at home and that her partner has been really stressed about work and money

Although the staff member does not have concrete evidence that DFV is occurring or has occurred, the information is enough to form a reasonable belief that Cynthia may be at-risk of DFV. The staff member does not currently have Cynthia's consent to share her information, but they may be able to share information about Ethan as a person of concern. To support this, the staff member uses the ACT RAMF to record their observations about Ethan's behaviour and the possible signs of physical violence observed in relation to Cynthia.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2.3. What information can be shared?

All **information, whether true or not, in any form and including an opinion and advice** can be shared under Part 3 of the DVA Act. This includes *sensitive information*. **Sensitive information** refers to information or an opinion about an **identified person**, or a person who is reasonably identifiable (including their personal and health information).

ⓘ Remember

Information and **sensitive information** are defined under the DVA Act. Sensitive information under other laws may be defined differently. Please refer to relevant legislation for current and accurate definitions.

Information is defined broadly, so that any information can be shared under the DFVISS if it is necessary for a protection purpose. Facts might include things that are absolute, such as the date a person of concern will be released from custody. An opinion might include a practitioner's assessment that the person of concern poses a serious risk of harm to others. This means that any information in any form can be shared as long as:

- The relevant **thresholds** for sharing information are met (see Chapter 2.2).
- Sharing information is not prohibited by the DVA Act (see Chapter 2.6 to understand if a 'relevant ground' applies).
- Sharing the information would **not breach** another law (see Chapter 9.1).

ⓘ Remember

Risk assessment is the process of identifying if a person is at risk of DFV and then determining the seriousness of that risk. Risk assessment relies on a structured professional judgement approach (see the ACT RAMF).

Because different agencies will hold different information, it is often necessary to share information to help assess and manage risk in a holistic way.

Protocol Requirement

- In identifying what information is relevant to share for a protection purpose, practitioners **must** rely on the **ACT RAMF.**

Practice Guidance

- Dealing with sensitive information has specific consent requirements (see Chapter 5 and 6).
- If information is de-identified, consent requirements for the DFVISS do not apply.
- Sometimes, ISEs may not be able to identify what information is risk relevant until the information has been collaboratively shared.
- The DFVISS allows ISEs to share information in this context, to support ISEs to identify what information is relevant to risk assessment – which *is* a protection purpose.
- For specific guidance on sharing information about a person of concern, see Chapter 5.2.
- Different laws define sensitive information differently. For guidance on other interacting laws, see Chapter 9.1.
- ISEs may also share employee information they hold, where this meets the requirements of the DFVISS.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2.4. How should information be requested and shared?

The DVA Act does not specify how information requests and sharing should occur, as the process of sharing information can be dynamic and at times, urgent. Because of this, information can be requested and shared both verbally and in writing. This ensures ISEs have **flexibility to coordinate and collaborate in the process of information sharing.**

ISEs should always respond to requests in a timely manner. Delays in information sharing may result in ISEs not meeting the aims of the DFVISS to prevent and reduce DFV, including risking the safety of victim-survivors.

Protocol Requirement

- Where a request has been identified as urgent, time sensitive *or* a serious risk (as per the ACT RAMF) has been identified, ISEs **must** respond without unreasonable delay.
- If an ISE has not responded to a request within a stated reasonable timeframe, the request is taken to be refused. The requesting ISE may therefore notify the Information Sharing Coordinator (see Chapter 4.3).
- While it is up to ISEs to decide how they manage or centralise information sharing requests, ISEs need to ensure that their own internal practices facilitate timely information sharing, especially in urgent, time sensitive, and serious risk scenarios.

Practice Guidance

- Information can be requested and shared both verbally and in writing.
- ISEs should always respond to requests in a timely manner. When a timeframe has not been specified, ISEs are generally required to do the activity as soon as possible and as often as needed.
- ISEs should coordinate and collaborate on an information sharing request to agree on a timeframe to respond. However, the requesting ISE should ultimately set a reasonable timeframe for when the information is needed by, including the level of urgency.
- When requesting information, an ISE should explain why the information is relevant to a protection purpose.
- The responding ISE should identify what information it holds is relevant to the request. ISEs must rely on the ACT RAMF to help determine what is relevant (see Chapter 2.3).
- Regardless of how information is requested or shared, record keeping requirements apply (see Chapter 7).
- ISEs must record when they are relying on Part 3 of the DVA Act to share information, or when they have received information under Part 3 (refer to Protocol Requirements in Chapter 7.7).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

How to request information under the DFVISS

Figure 2 describes how ISEs can make a request for information under the DFVISS.

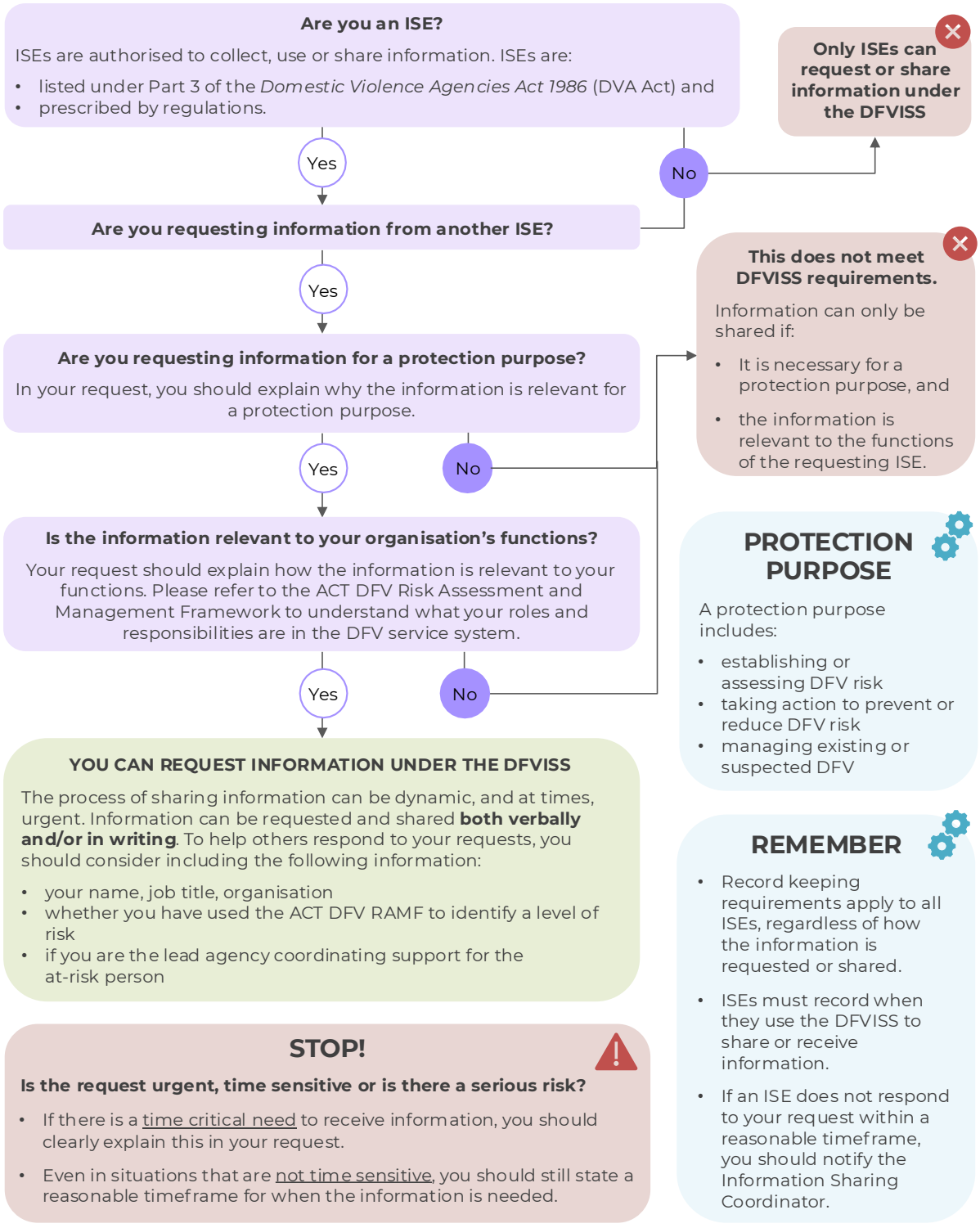


Figure 2: Flowchart - How to request information under the DFVISS

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Responding to a request for information under the DFVISS

Figure 3 describes how ISEs should respond to requests for information under the DFVISS.

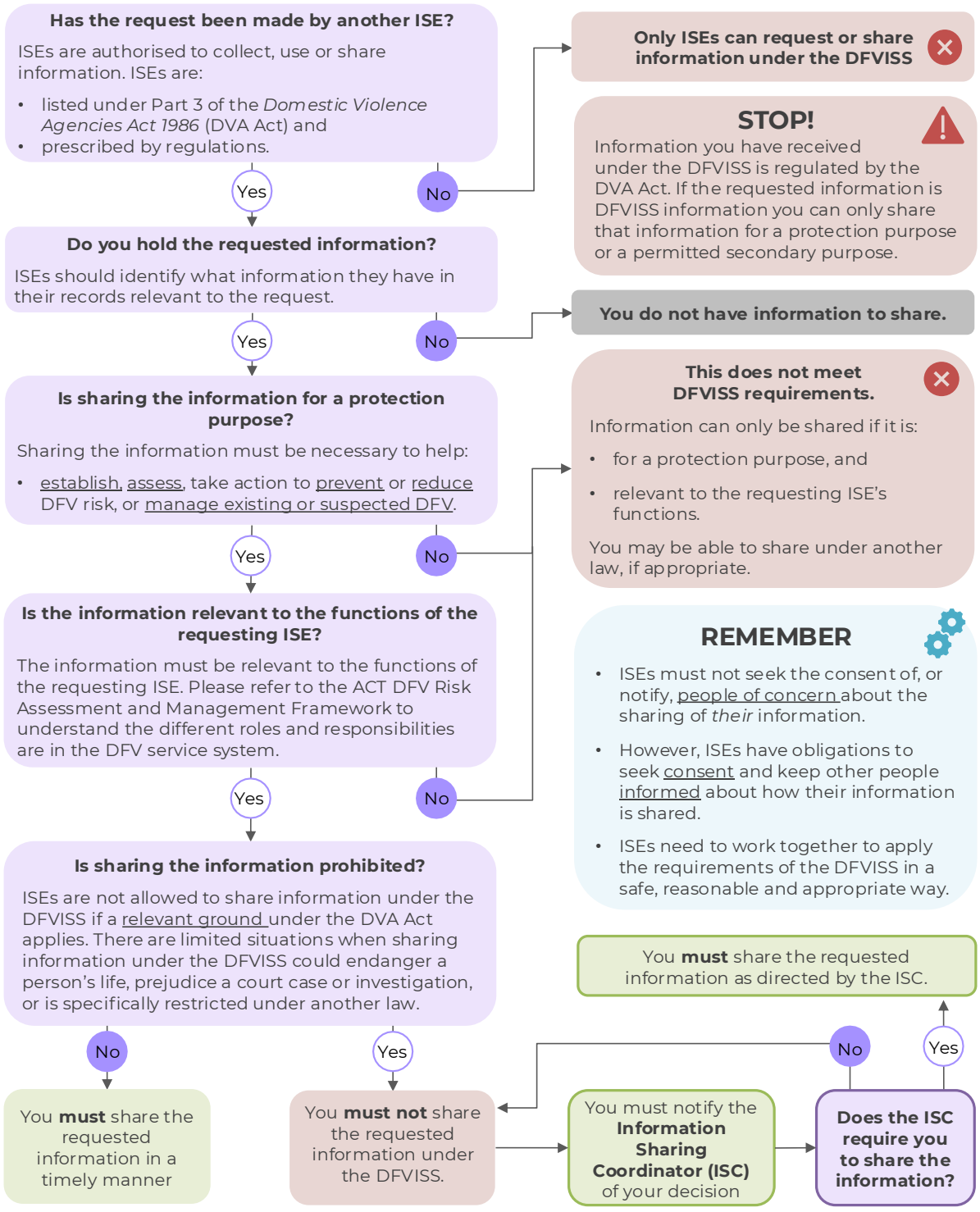


Figure 3: Flowchart - Responding to a request for information under the DFVISS

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2.5. How can information be used?

Once information has been shared under the DFVISS, the DVA Act regulates how that shared information can be further disclosed or used.

Key Points

- Information obtained under the DFVISS can generally only be used for a **protection purpose**.
- On-sharing of victim-survivor information must not occur without the person's consent, unless an exception applies. See Chapter 6 for more information.
- However, there are a limited number of scenarios where information obtained under the DFVISS can be used or disclosed for a purpose *other than* a protection purpose (a **secondary purpose**).
- If an ISE is a **restricted entity**, the **restricted entity declaration** will specify the protection purposes that apply to the restricted entity (see Chapter 3.1).

ⓘ Remember

Chapter 2.2 summarises how a protection purpose is defined under the DVA Act, and provides practice guidance on how to determine if something is *necessary* for a protection purpose.

On-sharing of victim-survivor information

Under the DVA Act, information about at-risk people (victim-survivors) cannot be shared, or 'on-shared', without their consent unless an exception applies. This is a key part of the DFVISS, which seeks to support the agency and autonomy of victim-survivors, by ensuring their information is not used without their knowledge except in specified situations.

Just because a victim-survivor has consented to disclosure in relation to one ISE, does not mean that their consent applies indefinitely. Inappropriate disclosure or use of victim-survivor information may increase risk to a victim-survivor. Offences and penalties may also apply (see Chapter 10).

Consulting with a victim-survivor on how their information may be used under the DFVISS is critical to support their safety. This will help an ISE determine if sharing information meets the DFVISS requirements (see Chapter 2.2).

Practice Guidance

- If an ISE on-shares victim-survivor information, that ISE should inform either the original ISE that shared the information with them, or the lead agency coordinating support for the victim-survivor. This is to facilitate an effective multi-agency response.
- Victim-survivor information must not be on-shared to other ISEs, without the person's consent unless an exception specifically applies (see Chapter 6).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Dealing with information for a protection purpose

ⓘ Remember

Information sharing practices need to hold the person using violence in view. This is because a protection purpose fundamentally relates to assessing and managing risk of DFV. This purpose can be best achieved by focusing on the behaviours, actions and circumstances of the person using violence

Disclosing or using information for a protection purpose can include various actions. For example, dealing with information for a protection purpose can generally authorise ISEs to:

- request further information based on some information or an incomplete picture of risk
- screen or assess for DFV risk in a timely and accurate way
- conduct holistic and informed risk assessment and safety planning
- intervene early to stop violence escalating to crisis point
- reduce or manage the risk of DFV, including the risk of serious harm or lethality
- prevent crisis or escalation, rather than only responding to crisis
- develop integrated and collaborative responses to DFV risk across critical points of engagement with at-risk people and persons of concern.

The information contained in this Ministerial Protocol is not exhaustive. These examples demonstrate the breadth of actions that can be within scope of the DFVISS, among others.

Practice Guidance

- A protection purpose includes activities that support risk assessment and management practice described in the ACT RAMF. This includes information sharing that supports the breadth of RAMF activities, including when screening or identifying DFV risk, conducting risk assessments, and engaging in risk management practice (such as safety planning).
- The roles and responsibilities of organisations, services and workers outlined in the ACT RAMF will support ISEs to understand the scope of their functions, based on their level of specialisation.
- Refer to Chapter 2.2 for general practice guidance in understanding what may be considered as 'necessary for a protection purpose'.

Establish or assess risk

ISEs may use information collected and disclosed through the DFVISS to inform an evidence-based assessment of DFV risk, using the **ACT RAMF**. This may involve using or seeking information to:

- Enable risk screening, risk identification and risk assessment practices.
- Understand and track a person of concern's pattern of behaviour and circumstances (**perpetrator pattern mapping**) to inform an assessment of risk, the nature of that risk, and the likelihood of future violence and risk points. See Chapter 5.2 for further information on what is relevant when sharing information about a person of concern.
- Understand the full spectrum, presentation and impact of risk for each family member affected by the person of concern's violence, including children and young people. This impact will help determine the most appropriate short and long-term risk management options, including safety planning for each victim-survivor.
- Understand the level of risk at a point in time and monitor for changes in risk over time.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Practice Guidance

- Risk assessment is the process of identifying if a person is at risk of DFV and then determining the seriousness of that risk. Determining seriousness of risk is undertaken through a process of applying structured professional judgement (see the ACT RAMF).
- Processes for **establishing or assessing risk** (including risk screening, risk identification and risk assessment tools) are comprehensively provided for in the **ACT RAMF**. Depending on the specialisation or 'tier' of the ISE, different guidance and tools may apply.
- **Risk assessment** is an ongoing process that forms the basis of an effective response to domestic and family violence. It is critical to understand that risk can change markedly over time or even within a short time. Risk assessment will only be effective if it is reviewed and updated regularly.

Case Study 2: Sharing and using victim-survivor information for the purpose of risk assessment

Alex has engaged a specialist DFV service for support, as they are planning to leave their partner and are concerned about their safety. This service is an Information Sharing Entity under the Scheme and a Tier 3 agency under the ACT RAMF.

During discussions with the service, Alex discloses that they have been hospitalised several times for injuries resulting from their partner's violence. They describe their partner's behaviour and express concerns about further violence based on recent threats. However, Alex explains that they cannot remember every specific incident because the violence has been going on for so long and some details are unclear. They also advise the service that recounting these instances is distressing.

To support a comprehensive risk assessment, the service asks for Alex's consent to obtain their hospital records. Alex provides consent, and the service requests the information from Canberra Health Services (CHS) under the DFVISS.

CHS identifies the records that are relevant to this specific request and shares those records with the specialist DFV service. This information assists the service to better understand the nature and extent of the harm experienced by Alex and to undertake a more informed assessment of their risk and safety needs.

Taking action to prevent or reduce risk, and manage risk

Where an ISE has assessed that a victim-survivor is at risk of DFV or a person of concern is at risk of engaging in or further engaging in DFV, ISEs can use the information to prevent, reduce and manage the identified risk – this is referred to in the ACT RAMF as risk management practice. Using information in this way may look like:

- Referring a victim-survivor to a more specialised agency, as needed, to conduct further risk assessment and risk management
- Sharing information with another ISE, such as a perpetrator intervention service or specialist DFV service
- Developing a safety plan with the at-risk person
- Developing a risk management plan
- Arranging an intervention to disrupt the person of concern's use of violence
- Increase monitoring or investigation activity of the person of concern
- In serious risk cases, sharing information to collaborate with agencies to further assess, manage and respond to the risk posed by a person of concern
- Proactively sharing information with other ISEs who are engaged with the person of concern, and where possible with at-risk people, to enact risk management strategies.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Practice Guidance

- **Risk management practice** (including actions that may be taken to prevent, reduce or respond to risk) are described for in the **ACT RAMF**.
- More specialised ISEs are supported by the ACT RAMF in understanding how to make **risk management plans**. These plans outline the required actions of services and workers that need to occur, to contribute to safer outcomes for the at-risk person.
- Developing a **safety plan** is a critical part of risk management and planning, regardless of the level of risk. A safety plan outlines in advance a range of actions that an at-risk person can take in a crisis or emergency situation. It is important that the plan is developed in partnership with the at-risk person, as they know the risks, know what strategies have worked in the past and know what might place them at increased risk. Please refer to the ACT RAMF.

Case Study 3: Seeking information about a person of concern from mental health services (safety planning and risk management)

Justin and Meera have two children together and have recently separated. Prior to the separation, Justin was convinced Meera was cheating on him. He began monitoring her movements and recording her in their house without her knowledge. During this time, Meera became concerned about Justin's mental health due to what she perceived as increasing paranoia. Justin decided to seek mental health support through Canberra Health Services (CHS) mental health services. Aside from this engagement, Justin has no known criminal history and no other interactions with government services.

The Family Violence Safety Action Program (FVSAP) is supporting Meera and monitoring Justin. Through risk assessment processes, Justin has been assessed to pose a serious risk as a person using violence, demonstrating persistent patterns of fixation on Meera and their children.

Following the separation, Justin moved out of the family home. However, he continued monitoring Meera's movements without her knowledge. Meera suspected this was occurring because of the messages Justin was sending her. Over the following months, Justin's fixation on Meera continued. He eventually broke into the family home while no one was present and caused property damage. Police attended the scene and arrested Justin. Charges were laid but were later withdrawn due to insufficient evidence and Justin's lack of prior criminal history.

Meera tells FVSAP that she believes Justin may still be engaged with mental health services. With Meera's consent, FVSAP contacts CHS via email explaining the context of violence and requests information about Justin's diagnoses, treatment and engagement with services. FVSAP also requests that CHS proactively share information if Justin disengages from services or becomes non-compliant with prescribed medication, noting that either circumstance would escalate risk of harm to Meera. FVSAP explains that the information will be used to support safety planning with Meera and contribute to perpetrator pattern mapping.

In this instance, CHS is required to share the requested information. Both CHS and FVSAP are ISEs and the request meets the requirements for information sharing under the DFVISS. The requested information relates to the protection purposes of risk assessment and risk management, and it directly supports FVSAP's functions and service provision.

Even though the information is health information, CHS must not seek Justin's consent to share it, and Justin cannot be notified that his information has been shared. CHS informs FVSAP that Justin is subject to a community-based treatment order, has been diagnosed with schizophrenia, and is being managed by certain medications that are necessary to reduce paranoid thought patterns. CHS agree to proactively notify FVSAP if there is a change in Justin's presentation or compliance with mental health services.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Secondary purpose

An ISE can disclose or use information other than for a protection purpose in limited situations. These secondary purposes are specifically listed under Part 3 of the DVA Act and are summarised in **Table 4.**

Secondary Purpose – DVA Act	Practice Guidance
With the consent of the at-risk or connected person	If the at-risk or connected person consents, the ISE can share their information outside the operation of Part 3 of the DVA Act. • **Consent** – To understand what 'consent' is, see Ch 8.1. • **Notification requirements** still apply (see Ch 6.6).
If it is required or allowed under a territory law to lessen or prevent a serious and urgent threat to life, health or safety of an individual, or to public health or safety	This secondary purpose preserves an ISEs ability to flexibly share information obtained through the DFVISS under other Territory laws that require or allow information sharing for a serious or urgent purpose. • **Sharing information under other laws** (see Ch 9.2).
To comply with a mandatory reporting or reportable conduct requirement	Any information received under Part 3 of the DVA Act can be used to comply with mandatory reporting or reportable conduct obligations. • **Mandatory reporting and reportable conduct obligations** (see Ch 9.2). • **Notification requirements** (see Table 10, Ch 6.6) – Other laws, such as mandatory reporting laws, may restrict what information can be contained in a notification under the DFVISS.
To the extent required or allowed under another territory law, prescribed by a regulation under the DVA Act	• **Other territory law** – If another territory law has been prescribed, information under the DFVISS can be shared in accordance with the other prescribed law. ISEs should access the ACT Legislation Register to confirm what laws, if any, have been prescribed by regulation under the DVA Act.

Table 4: Understanding when information can be shared for a secondary purpose under the DVA Act

Practice Guidance

- If complying with one of the secondary purposes above, an ISE can share with a non-ISE.
- If an ISE discloses or uses information for a secondary purpose, they must tell the **Information Sharing Coordinator** (see Chapter 4.3).
- If the information is about an at-risk or connected person, that person must also be told about the use or disclosure of their information unless an exception applies (see Chapter 6.6).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Case Study 4: Secondary purpose (consent) – sharing DFVISS information to a non-ISE in a multi-agency information sharing forum

Victim Support ACT (VSACT) requests information about a victim-survivor from Children, Youth and Families (CYF). VSACT and CYF are both ISEs. VSACT receives this information and tags it as DFVISS information in their information management system. In a multi-agency meeting of the Family Violence Safety Action Program (FVSAP), VSACT wants to share this information with a member who is not an ISE.

The DVA Act regulates how VSACT can use or disclose information it has received under the DFVISS. As VSACT wants to share the information with a non-ISE, they can only do so if a secondary purpose applies. VSACT works with CYF to obtain the consent of the victim-survivor to share their information with the non-ISE, as well as discussing with the victim-survivor their views on being kept informed about what happens with their information. The victim-survivor advises they do not want to be notified unless their information is shared with ACT Policing.

Now that VSACT have shared this information, they must, in writing, tell both the Information Sharing Coordinator (within 14 days) and CYF that they shared DFVISS information for a secondary purpose.

Case Study 5: Secondary purpose (emergency) – Sharing DFVISS information to lessen or prevent serious harms

Claudia's partner, Declan, is known to the Family Violence Safety Action Program (FVSAP) and has been the subject of ongoing risk monitoring over several years. Through its work with Claudia and information received from multiple Information Sharing Entities (ISEs), FVSAP has accumulated a range of intelligence about Declan and his risk profile.

Information held by FVSAP identifies a history of threats involving explosive devices and a long-standing interest in constructing improvised devices. More recently, Housing ACT shared information under the DFVISS following a property inspection. Staff reported that Declan became highly agitated when they attempted to inspect the garage, where they observed a large number of tools, equipment and partially assembled objects. Separately, another ISE advised FVSAP that Declan’s mental health had significantly deteriorated and that he had become increasingly fixated on grievances against government institutions and "the system".

One day, Claudia contacted FVSAP after receiving a series of disorganised and distressed messages from Declan. During the conversation, she mentioned that Declan had recently cleared out the garage and removed something he had been building, loading it into his vehicle. He said he wasn’t coming back.

Viewed in isolation, Claudia's information did not indicate an immediate serious threat. However, when considered alongside the information already held by FVSAP and the information received from other ISEs, it became a critical piece of a much larger risk picture. The combined information suggested a credible possibility that Declan had constructed and removed a device capable of causing significant harm to members of the public.

FVSAP assessed that the risk extended beyond DFV and may involve a serious threat to public health and safety. To enable an urgent response, FVSAP shared all relevant information with Police for a secondary purpose under the DFVISS, including information originally received under the DFVISS. This allowed Police to take appropriate enforcement actions.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

2.6. When you must not share information

ISEs are not allowed to share information if:

- a relevant ground under the DVA Act applies, or
- it would breach another law (see Chapter 9.1)

An ISE must not share information if a **relevant ground** under Division 3.3 of the DVA Act exists. This is a specific provision of the DVA Act, and it recognises there are limited situations where sharing information under Part 3 cannot occur due to other policy reasons. A relevant ground exists if the disclosure:

- **Contravenes a requirement for information sharing** under the DFVISS (e.g. sharing the information is without consent of a victim-survivor, and no exception applies, or sharing information would elevate risk and therefore be contrary to a protection purpose)
- Could **endanger a person's life or physical safety** (e.g. if sharing the address of the victim-survivor could reveal their whereabouts and risk their safety)
- Could **prejudice an investigation** (e.g. sharing information that could get back to a person involved in criminal activity)
- Could **reveal the existence or identity of a confidential source of information that helps enforce or administer a law** in the ACT (e.g. sharing information that could reveal the identity of a person who gave information on the understanding their identity would be confidential. In this situation, it is usually the *source* – rather than the information– which is confidential)
- Could **prejudice the effectiveness of lawful methods and procedures that aim to prevent, detect, investigate or deal with a – possible – contravention of an ACT law** (e.g. for something to negatively affect lawful methods and procedures, it will generally need to reveal something that is not obvious or well known by the public. This could relate to criminal and other investigations, such as tax or regulatory matters)
- Could **prejudice a court or tribunal proceeding, including a coronial inquest or inquiry** (e.g. if the information could lead to witness tampering, or the information was cited as evidence in a closed court proceeding to protect the administration of justice or the privacy of a victim-survivor)
- Could **contravene an order of a court or tribunal** (e.g. sharing information that may have been supressed or otherwise restricted for sharing in a legal proceeding)
- Could **be contrary to the public interest**. While the public interest test in freedom of information laws is not applicable to the DVA Act, ISEs are encouraged to refer to the Australian Information Commissioner Freedom of Information Guidelines for guidance on what 'public interest' generally refers to.

ⓘ Remember

Information that relates to investigations, inquiries, court orders or legal matters is not automatically excluded under the DFVISS. ISEs must consider the impact of sharing the information to decide if it is excluded. For example, would sharing information relating to a coronial inquest prejudice the inquest in a particular circumstance? This assessment is based on information that is known to the ISE at the time.

Practice Guidance

- If you refuse to share information under the DFVISS, you are required to notify the Information Sharing Coordinator (see Chapter 4).
- ISEs may wish to seek legal advice relevant to their specific context, and the information they hold.
- Client legal privilege and the privilege against self-incrimination continue to apply to the DFVISS.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

3. WHO IS ALLOWED TO SHARE INFORMATION UNDER PART 3?

Chapter 3 explains who is authorised to use the information sharing powers of the DFVISS, and who those entities are permitted to share information with. Over time, more organisations, services and agencies may become ISEs.

Key Points

- Only entities that are specifically prescribed under Part 3 of the DVA Act are allowed to share information under the DFVISS.
- An information sharing entity (ISE) includes the Information Sharing Coordinator (see Chapter 4).
- The responsible Minister can declare other entities to become ISEs under the DFVISS.
- The DVA Act also permits a police officer to disclose any information to an **approved crisis support organisation**, to enable that organisation to assist a victim-survivor.
- ISEs that obtain information under the DFVISS may be able to share information with non-ISEs for a secondary purpose. This is described in Chapter 2.5.
- For information not obtained under the DFVISS, an ISE may choose to engage in information sharing under other existing and applicable laws.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

3.1. Who is an ISE under Part 3?

An ISE is an agency, service or organisation specifically allowed to collect, use or disclose information under Part 3 of the DVA Act.

The DVA Act specifies which entities are ISEs. This includes the Information Sharing Coordinator and other entities including education providers, corrective services, emergency services, housing, police and others.

The DVA Act provides a process for other agencies to become ISEs, once approved by the responsible Minister. If the Minister declares an entity to be an ISE, the Minister may state the protection purposes that apply to that entity. If entities are declared for only a specific protection purpose, those entities become **restricted entities** and can only use the DFVISS for the specific purpose(s) named in their declaration. If an entity is declared without a specific protection purpose, they are a full ISE under the DFVISS, and all protection purposes apply to them.

Practice Guidance

- For a list of **current ISEs**, please refer to the DVA Act, relevant delegations (if applicable) and relevant legislative instruments prescribing additional ISEs.
- To support the administration of the DFVISS, you can also access a summary list of ISEs online**,** which is updated from time to time.
- **When sharing information with a restricted entity**, you must only disclose information that is relevant to their stated protection purposes named in the legislative instrument prescribing them as a restricted entity (if applicable). This can be accessed on the ACT Legislation Register.

3.2. Who can ISEs share information with?

An ISE can only share information for a **protection purpose** under Part 3 with:

- **another ISE** (including the Information Sharing Coordinator), and
- an **at-risk person** (this is limited to sharing information *about* a person of concern, see Chapter 5.4).

ⓘ Remember

ISEs are not allowed to share information with a person of concern (see Chapter 5.1). This is an important requirement and safeguard of the DFVISS. Offences and penalties may apply (see Chapter 10).

The DVA Act also permits a police officer to disclose any information to an **approved crisis support organisation**, to enable that organisation to assist a victim-survivor.

3.3. Sharing with non-ISEs

There are organisations in the ACT, interstate, and nationally that may hold risk relevant information and are not ISEs under the DFVISS.

If an ISE wants to share information it has received under the DFVISS with a non-ISE, it must rely on a permitted secondary purpose under the DVA Act (see Table 4, Chapter 2.5).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

4. THE INFORMATION SHARING COORDINATOR

Chapter 4 describes the independent and expert oversight role of the Information Sharing Coordinator (ISC) in the DFVISS. The ISC has various functions prescribed by the DVA Act, which support the efficient and safe information sharing.

Key Points

- The ISC is a specific role created by Part 3 of the DVA Act. It provides independent oversight over the operation of the DFVISS and has the power to compel information sharing in certain situations.
- A key part of the ISC's oversight function involves reviewing all instances where an ISE refuses to share information under the DFVISS. The ISC ensures that refusals to share information (Chapter 2.6) align with the requirements of the DFVISS.
- The ISC can require ISEs to share information, if they have incorrectly refused a request for information sharing (see Chapter 4.2). This is necessary to overcome historical cultural and systemic barriers to information sharing in the ACT.
- There are specific scenarios where ISEs will be required to communicate with the ISC under the DFVISS. This relates to when an ISE refuses to disclose information under the DFVISS, or an ISE uses or discloses information for a secondary purpose.
- ISEs need to understand the role of the ISC, and how they are required to interact with them from time to time. This is summarised in Chapter 4.3.
- Aside from the formal oversight and arbitration functions of the ISC, it also has an essential role to facilitate information sharing across the service system by supporting all ISEs to build their own operational capacity under the DFVISS. ISEs should seek guidance from the ISC to support a collaborative approach to information sharing.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

4.1. The role of the ISC

The Information Sharing Coordinator (ISC) is an independent role created by Part 3 of the DVA Act. The role and functions of the ISC described in the DVA Act are to:

- Facilitate information sharing between ISEs, including by requiring ISEs to share information in certain situations;
- Identify and take actions for a protection purpose; and
- Any other function given to the ISC under the DVA Act.

Taking actions for a protection purpose

The DVA Act empowers the ISC to be able to take actions for a protection purpose. The ISC can consider any information disclosed to it under Part 3 when deciding what actions it may take. Examples of actions an ISC may take include:

- **seeking information** from an ISE to help decide the most appropriate action to take.
- **giving advice** to an ISE about appropriate actions the ISE can take.
- **coordinating** ISEs in taking actions under Part 3 (e.g. holding a coordination meeting with ISEs).
- **assisting** the at-risk person and their family members (e.g. giving advice, arranging supports).
- **referring** the at-risk person and their family members to a government or non-government entity for further advice and support.

When deciding what actions it should take, the ISC must take into account certain requirements set out by the DVA Act. These are summarised in **Table 5.**

ISC must take into account:	Practice Guidance
The safety and protection of the at-risk person.	• **Necessary for safety and protection** – Refer to practice guidance in Ch 6.5.
The views of the at-risk person, where safe, reasonable and practicable to seek their views	• **Seeking views** – This is central to good risk assessment and management practice, which is contemplated by the principles for information sharing in this Ministerial Protocol (see Ch 1.3). • **Safe, reasonable and practicable** – the ISC should refer to the practice guidance in relation to who should seek consent, and when it is safe, reasonable and appropriate to seek consent (see Ch 6.2 and 6.3).
The seriousness of the circumstance	• This should be considered with reference to a risk assessment under the **ACT RAMF**.
The personal factors for at-risk people	• **Personal factors** – When exercising a function under the DFVISS in relation to an at-risk person, all ISEs (including the ISC) must consider specific personal factors prescribed by legislation for certain cohorts (see Ch 8.4).
Anything else prescribed by regulation	• To see if a regulation is in force under section 16AH(d), please refer to the ACT Legislation Register.

Table 5: What the ISC must take into account when considering taking action for a protection purpose

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

4.2. When can the ISC require information sharing?

The ISC can require you to disclose the requested information if they reasonably believe that:

- The information is relevant to the **functions of the ISE** who is seeking the information (see Chapter 2.2);
- The disclosure is necessary for a **protection purpose** (see Chapter 2.2); and
- A relevant ground under the DFVISS does not apply and sharing information would not breach another law (see Chapter 2.6).

If the above conditions are met, the ISC can require you to share the information. In this case, the ISC must give you a written notice, and you must comply with that notice.

4.3. How will ISEs interact with the ISC?

There are 2 scenarios where an ISE must communicate with the ISC and provide them with certain information. This is summarised in **Table 6**:

Scenario	When you must notify the ISC	What you must tell the ISC	How to tell the ISC	Protocol Requirement: Timing
Refusal	If you refuse to disclose information in response to another ISE's request[1]	• The name of the requesting ISE • The nature of the information requested • The relevant ground you did not disclose	In writing	The ISE must notify the ISC without unreasonable delay
Secondary purpose	You use or disclose information for a secondary purpose	• About the use or disclosure[2]	In writing	The ISE must notify the ISC as soon as reasonably practicable, but not later than 14 days

Table 6: Requirements for communicating with the ISC

Practice Guidance

[1] If an ISE **fails to respond to a request to share information** within a stated timeframe, the request is taken to be refused. The requesting ISE may notify the Information Sharing Coordinator of the failure to respond, and the ISC may require the sharing of information.[1] If an ISE **fails to respond to a request to share information** within a stated timeframe, the request is taken to be refused. The requesting ISE may notify the Information Sharing Coordinator of the failure to respond, and the ISC may require the sharing of information.

[2] When you tell the ISC about a secondary use or disclosure, you must comply with any other relevant law that you have dealt with the information under. For example, if an ISE discloses information to comply with a mandatory reporting requirement under the *Children and Young People Act 2008*, the ISE is restricted under that law from disclosing certain information. This means the ISE must not breach these protections in the process of telling the ISC about the use or disclosure.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Case Study 6: ISE refused request to share information under the DFVISS based on a relevant ground to not disclose

ACT Policing receives a request for information under the DFVISS from a non-government school within the ACT. The school requests information about George, a father of one of the students, whom the family have a family violence order against. George is known to the police for his alleged involvement in organised crime. The student told their teacher they were scared dad would turn up to the school with his “friends” and cause trouble. Because of this, the school requests information from ACT Policing about George’s associates, to help identify if they appear near or on school grounds.

ACT Policing review the request and conclude that sharing the information is not allowed as they reasonably believe it could prejudice an investigation. This is a relevant ground to not disclose information under the DFVISS. They consider the impact of sharing the information to decide that it should be excluded in this situation, due to other factors of the investigation.

ACT Policing notifies the Information Sharing Coordinator (ISC) in writing about their decision to not share the information to the school and why. The ISC considers the refusal and is satisfied that a relevant ground for not disclosing the information exists. The school reaches out to the ISC seeking advice on possible next steps to ensure the safety of the at-risk student. The ISC facilitates a service coordination meeting with ISEs in response.

Despite ACT Policing not sharing information, the non-government school shared the information they held with ACT Policing as part of making their request. This meant that ACT Policing is able to use this information to consider their approach to support risk management.

Case Study 7: ISC compels ISE to share information

Shane receives NDIS-funded supports through a disability service provider (an ISE) and relies on his brother Jared for day-to-day assistance, including transport and attending appointments. The disability service provider holds information about both Shane and Jared, including concerns recorded by staff that Jared closely monitors Shane's activities, frequently requests information about Shane's support arrangements, and has become frustrated when staff speak with Shane directly.

At a medical appointment with Canberra Health Services (CHS), a practitioner observes Jared repeatedly interrupting Shane and answering questions on his behalf, while Shane appears reluctant to express his own views. The practitioner forms a belief that Shane may be at risk of DFV and seeks information from the disability service provider to help establish or assess that risk under the DFVISS.

The disability service provider refuses the request, stating: "The information was collected as part of our disability support services, and we are concerned that sharing it may breach our confidentiality obligations to clients."

The provider notifies the Information Sharing Coordinator (ISC) in writing of its decision and reasons.

The ISC reviews the refusal and determines that:

- the information is necessary to establish or assess DFV risk
- the information is relevant to CHS's functions under its responsibilities in the ACT RAMF
- no ground exists to refuse disclosure in these circumstances

The ISC directs the disability service provider to disclose the requested information and explains that the DFVISS authorises the sharing of relevant information where the legislative requirements are met and that victim-survivor safety is the paramount consideration.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

5. SHARING INFORMATION: PERSON OF CONCERN

This Chapter provides guidance on how information sharing about a **person of concern** works under the DFVISS, including considerations for identifying the person of concern, and sharing information to build a picture of risk.

The DFVISS will be most effective when ISEs focus on sharing information about people who use violence to assess and manage the risk that they pose. It is for this reason Part 3 of the DVA Act has been introduced to remove information sharing barriers and address institutional cultures which emphasise privacy and secrecy protections, particularly in relation to people who use violence.

ⓘ Remember

- A **person of concern** is someone who has engaged in, is engaging in, or is at risk of engaging in, DFV. This could be an adult, child or young person.
- Most organisations and services do not work directly with people to change their use of violence. However, many practitioners engage daily with people who may be using DFV while presenting with other needs.
- Given the prevalence of DFV in the community, it is likely that you work with people using DFV even when this is not the primary reason for service contact. As a result, your service may hold a wealth of risk-relevant information, that can support risk assessment and management practices.

Key Points

- An ISE **must not** seek a person of concern's consent to collect, use or disclose their information, including personal and health information under the DFVISS. This does not limit the ISEs ability to deal with their information under the DFVISS (see Chapter 5.1).
- The consent requirement does not change usual eligibility, intake and assessment processes for organisations that work with people who are, or may be, using violence (see Case Study 8, Chapter 5.1).
- ISEs **must not** inform a person of concern if they have collected or used information – including their own – under the DFVISS (see Chapter 5.1). Offences and liability may apply (see Chapter 10).
- Sharing information to build a picture of risk of a person of concern (e.g. **perpetrator pattern mapping**) will be a key part of sharing information for a protection purpose under the DFVISS (see Chapter 5.2). This will support collaborative and proactive system responses, as opposed to a service system that only responds in, or after, an incident or crisis.
- Where an ISE is uncertain about the **identification or misidentification** of the person of concern and at-risk person, information sharing will be essential to identify the person most in need of protection; the 'primary victim' (see Chapter 5.3). ISEs should refer to the specific guidance on misidentification and determining the primary aggressor in the **ACT RAMF**.
- An ISE who believes a person has been **misidentified** as a person of concern or at-risk person under the DFVISS must take reasonable steps to correct the misidentification, and apply the requirements of the DFVISS. See also record keeping obligations in Chapter 7.6.
- ISEs **must rely on the ACT RAMF** to engage in safe and informed information sharing practices.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

5.1. Consent is not required

ISEs **must not seek the consent of a person of concern** to collect, use or disclose information about them. This is a key requirement of Part 3 of the DVA Act to overcome the practical and cultural barriers to sharing information about people who use violence.

Additionally, ISEs **must not tell a person of concern that information has been dealt with** under the DFVISS. This is another general safeguard of the DFVISS to promote the safety of victim-survivors. Offences and liability may apply if ISEs breach this requirement (see Chapter 10).

A person who uses violence may identify where information originated from, or that information about them has been shared, and raise this with staff in an ISE. If the information was shared under the DFVISS, the ISE cannot tell the person using violence that their information has been shared. These scenarios should be considered on a case-by-case basis, and if you are unsure how to manage the situation, seek secondary consultation with your manager, the Information Sharing Coordinator or a specialist DFV service if appropriate.

Practice Guidance

- ISEs that work directly with people who use violence cannot tell a person of concern when their information has been specifically dealt with under the DFVISS.
- However, ISEs can provide general information about the laws and policies that they operate under, including the DFVISS. This can support transparency of service provision to a person of concern, without breaching the requirements of the DVA Act and escalating risk.
- ISEs that work with people who use violence about their use of violence – such as through behaviour change programs – may sometimes need to discuss risk information and disclosures directly with the person using violence. This process can be managed by specialist services sharing information through other information sharing pathways.
- Violence used by children and young people may require distinct responses. Please refer to the ACT RAMF for more information on children and young people who use violence. If you are unsure if child or young person is a person of concern, seek secondary consultation within your ISE or the Information Sharing Coordinator.

Case Study 8: Where workers do not use the DFVISS to support safe engagement with people using violence

A case manager in a Men's Behaviour Change Program (MBCP) is working with Julian under a court ordered program. Julian is using violence in his relationship. As part of intake and assessment, Julian is made aware that the service provider has obligations under various laws where they may need to disclose his information without consent, to manage certain risks. This is a normal part of the eligibility process and does not breach DFVISS requirements.

The MBCP receives information about Julian's use of violence, through the partner contact or family safety contact function. The information they receive reveals that Julian has been minimising and hiding recent violent behaviours. Julian's case worker is notified of this information, and the case worker discusses this risk information directly with Julian. Because the information relates to compliance under Julian's court order, the case worker shares this information with Corrections and informs Julian that the information has been shared by the MBCP.

In this example, the service provider is **not** relying on the DFVISS to share or receive information – for this reason, it is able to tell Julian about the risk information in an appropriate way to promote his accountability, and further share information to another organisation without making the victim-survivor "responsible" for the system response. This highlights how the DFVISS should be utilised as a tool for information sharing when appropriate to do so, but the DFVISS does not govern all functions of a service provider only because it is an 'ISE'.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Case Study 9: When workers cannot tell people using violence that their information has been shared under the DFVISS

The case worker in the MBCP working with Julian later receives information from the Family Violence Safety Action Program (FVSAP), which helps co-ordinate multi-agency responses to serious risk DFV cases in the ACT. FVSAP informs the MBCP case worker that they have information that the violence is escalating, but the victim-survivor has not disclosed this through the partner contact function because they are afraid this will further escalate the violence. FVSAP shares this information with the MBCP case worker under the DFVISS.

Because the MBCP has received this information under the DFVISS, they cannot tell Julian that they are aware of that information. Instead, the MBCP case worker and FVSAP work together as part of risk management planning to identify appropriate interventions and responses to Julian to promote his accountability, while working with the victim-survivor to prevent escalation.

Case Study 10: Where sharing information for a secondary purpose under the DFVISS may support safer responses

Because FVSAP is working with Julian's partner on an ongoing basis, they become aware that the violence has continued to escalate very seriously, and FVSAP is concerned that the victim-survivor is now at serious risk of serious harm or lethal violence.

In this scenario, FVSAP informs the MBCP case worker that their risk management plan needs to be enacted to disrupt the violence, and both services work together to notify ACT Policing about the serious and escalating harm. In this scenario, both FVSAP and the MBCP decide it is necessary to share some information with Julian directly, including how his information has been dealt with, so that Julian does not solely 'blame' the victim-survivor for police involvement.

In these scenarios, certain information was shared with Julian for a permitted secondary purpose under the DFVISS, by relying on other laws that permit information sharing in serious and urgent circumstances (see Chapter 2.5). This was the best decision to support a safer system response in this specific circumstance.

5.2. What information is relevant?

The relevance of information is not always clear when seen in isolation. This is particularly true about the behaviours of people using violence. Sharing information to help understand these patterns and using a risk assessment framework to predict when violence might escalate is a key part of risk assessment and management practice. Sharing information can also help **identify the person of concern**, so that information can be shared safely (see Chapter 5.3).

Recording your professional observations about a person of concern and sharing information to build a profile of a person of concern (sometimes called **perpetrator pattern mapping**) can be necessary for a protection purpose. **Perpetrator pattern mapping** is the process of identifying and assessing the specific behaviours of a perpetrator, their patterns of behaviour, and the impact these have on a victim-survivor.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Protocol Requirement

- In determining what information is relevant to share for a protection purpose, practitioners **must** (where relevant) rely on the **ACT RAMF**.

Practice Guidance

- The ACT RAMF supports organisations and workers to identify risk, using dedicated tools for recording professional observations about a person using violence, or a person you suspect may be using violence. This information can help identify, assess and respond to DFV risk.
- Sometimes, ISEs will need to record and share information to help identify whether the information is risk relevant, to help establish and assess DFV risk.
- Details about the personal needs and circumstances of a person of concern are risk-relevant information that can inform your understanding of DFV risk at a point in time. This may include their personal and health information (see Chapter 2.3).
- Responding ISEs should identify what information it holds is relevant to a request to share information, using the ACT RAMF.
- What is relevant will also depend on the function(s) of the ISE seeking the information (see Chapter 2.2).
- If unsure what information is relevant to share, seek secondary consultation internally (within your ISE), the Information Sharing Coordinator, or externally with a specialist family violence ISE. Remember that you can share information in a de-identified way (see Chapter 2.3).

Case Study 11: Determining what information is relevant – Health services sharing information with a specialist DFV service

John and his ex-partner Melissa have 2 children. After their recent separation, John was convicted of a drink driving offence and was ordered to attend an alcohol and other drug service run by Canberra Health Services (CHS) as part of his Good Behaviour Order.

During a scheduled meeting with a CHS worker, John explains he has been struggling since his separation, and that he wants to reconcile with Melissa. He mentioned he has been hanging outside her workplace to try and see her. He also mentioned he thinks she is seeing someone else, because he has noticed a new car in the driveway of the family home and he is worried about how this is impacting his children. John explained that this stress has been causing him to drink more frequently. John presents as a calm but disorganised person who reports that he is trying to get his life 'back on track' so that he can be with Melissa and his kids.

The Family Violence Safety Action Program (FVSAP) is working with Melissa. Melissa has disclosed a long history of DFV in her relationship with John. FVSAP has identified John as a serious-risk person of concern, based on the information available to them. As a result, FVSAP requests information from CHS about John's substance use, including any other information available to CHS relevant to assessing and managing DFV risk. FVSAP disclose to CHS that John has been identified as a high-risk person of concern, and that they are concerned he may be stalking or monitoring Melissa and the children.

CHS is required to identify and share information that is relevant to a protection purpose. Under the ACT RAMF, stalking behaviours, fixation and substance misuse are all risk factors for violence. CHS reviews their file on John and identifies the above information that John disclosed to CHS. CHS is required to share this information, and discloses it to FVSAP.

CHS does not seek John's consent to share his personal and health information, because they are not permitted to do so. CHS does not tell John that they have dealt with his information under the DFVISS, following the requirements of the Scheme.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

5.3. Identifying the person of concern

Key Points

- ISEs may encounter a scenario where a person of concern openly presents themselves as the victim, or a police or other service response has misidentified the victim-survivor as the person of concern.
- Correctly identifying who is the person of concern is an essential part of safe information sharing.
- People using violence that are incorrectly identified as victims can use their victim status to further harm and control the true victim-survivor, as well as use systems to perpetrate more violence.

ⓘ Remember

- ISEs will sometimes need to assess if someone is the at-risk person or the person of concern (see Chapter 2.2). This is because different consent requirements apply depending on who you are sharing information about.
- In some instances, a person may be identified and assessed as a person using violence for an incident of domestic and family violence, and also a victim-survivor in that, or past, incident(s). These scenarios are complex, and proper identification practices conducted or supported by a specialist DFV service will be essential to supporting a safer system response.
- Misidentification of victim-survivors as the person using violence is a significant and well-documented issue for Aboriginal and Torres Strait Islander peoples, occurring at disproportionately higher rates due to systemic bias, over-policing and the failure of services to recognise contextual risk. These factors heighten immediate risk and escalation of harm, as well as entrench long-term intergenerational impacts on individual and community health.

Some people using violence will report being victim-survivors, or a legal or other system response has misidentified them as the victim. A person using violence can openly present themselves as the victim to manipulate services, including police. Presenting in this way is also consistent with 'victim stance' thinking that many persons of concern adopt to justify and excuse their behaviour.

Misidentification can occur when the focus is on a single incident, rather than taking into account prior history and the context for a violent incident.

Misidentification may also occur where a victim-survivor uses self-defence or violent resistance during an incident. In practice, this usually refers to a situation where police respond to an incident and **misidentify who is the person most in need of protection.** Proper identification practices mean relying on an evidence-based risk assessment framework to identify the primary aggressor. The primary aggressor is the person who poses the most serious and ongoing threat to safety. The primary aggressor is a person of concern under the DFVISS.

Protocol Requirement

- If an ISE reasonably believes a person has been misidentified as a person of concern or at-risk person under the DFVISS, the ISE must take reasonable steps to determine the 'primary aggressor' to safely apply the requirements of the DFVISS.
- If an ISE is taking steps to determine the 'primary aggressor' when exercising a function under the DFVISS, it must rely on the relevant guidance in the **ACT RAMF**. This guidance generally includes documenting your observations, proactively seeking information, recording your rationale on assessing who is the primary aggressor or alternatively recording your uncertainty if you are unable to decide at that time.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Practice Guidance

- For the purposes of the DFVISS, the 'primary aggressor' of domestic and family violence is the person of concern.
- All ISEs should, where possible and appropriate, assess for the correct identification of the person of concern prior to sharing information under the DFVISS.
- Misidentification may arise as an information sharing issue when:
  - ISEs disagree over who is the primary aggressor (that is, person of concern) and/or primary victim (that is, at-risk person).
  - There are cross-allegations of violence, including mutual protection orders.
  - A police response has charged an at-risk person with an offence, in relation to the person of concern.
- If ISEs disagree over the identification or misidentification of parties, they should work collaboratively to seek further information and correctly identify the parties.
- Where disagreement persists, and if an ISE refuses to disclose requested information, the refusing ISE must inform the Information Sharing Coordinator (see Chapter 4.3).
- In more complex case scenarios (e.g. children or young people using violence), ISEs will need to engage collaboratively with other agencies to ensure that information is shared safely and appropriately.
- ISEs need to be aware of their record keeping requirements in relation to misidentification, in Chapter 7.6.

Case Study 12: Identifying the primary aggressor

Police attend an incident between Luke and his 19-year old son Malakai following reports of a physical altercation. On arrival, Police observe the following things:

- Luke has a visible injury to his face
- Malakai is upset and admits he hit Luke during the argument, while Luke is calm and speaks constructively with Police.
- Luke tells police that Malakai is violent and unpredictable, and that this is not the first time this has happened.

Following the incident, Malakai contacts a specialist DFV service. Using the ACT RAMF, the service identifies indicators of ongoing violence and coercive control by Luke and assesses Malakai as the primary victim (the 'at risk' person under the DFVISS). With Malakai's consent, the service shares relevant information with ACT Policing under the DFVISS. Housing ACT also shares information about Malakai previously seeking emergency accommodation after being locked out of the family home by Luke.

Using the information shared by other Information Sharing Entities (ISEs), ACT Policing DFV officers undertake a further risk assessment informed by the ACT RAMF. ISEs are required to use the ACT RAMF when using the DFVISS. Considering the broader pattern of behaviour, rather than the single incident alone, Police determine that Luke is the primary aggressor and poses the most serious and ongoing risk to safety and wellbeing. Police conduct further inquiries which reveal that Malakai was acting in self-defence, and the charges were later discontinued.

This case study demonstrates how information sharing under the DFVISS can support more accurate risk assessment, prevent misidentification of victim-survivors, and improve responses to domestic and family violence.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

5.4. Sharing information with an at-risk person

ISEs are allowed to disclose information about a person of concern to an at-risk person if the disclosure is **necessary for a protection purpose and no relevant ground under section 16 exists.** This is important to support at-risk persons to manage their safety or the safety of their family.

However, sharing information about a person of concern with an at-risk person requires careful consideration. This is especially the case where the context of violence may make it unsafe or inappropriate to share the information directly with the at-risk person. This includes scenarios where:

- there is history of controlling behaviours, stalking, monitoring or technological facilitated abuse, such as using tracking software or accessing the victim-survivor's phone, emails or other personal information.
- the at-risk person and person of concern are still in a relationship or residing in the same home.
- the person of concern knows the at-risk person is engaged in services with the ISE.
- the person of concern may threaten, harass, intimidate or otherwise coerce the at-risk person into divulging information to them.

There may be occasions where disclosing information to an at-risk person about the person of concern could prejudice an ongoing investigation or legal proceeding. In that scenario, sharing information under the DFVISS is not permitted (see Chapter 2.6). Less specialised ISEs should work collaboratively with specialist DFV services when deciding if it is safe and appropriate to share information directly with the at-risk person.

Practice Guidance

- Sharing information about a person of concern directly with an at-risk person should usually be done by ISEs that have specific skills in DFV risk assessment and management. This will typically be Tier 2 and Tier 3 organisations and workers, as described in the **ACT RAMF**.
- Before sharing information with an at-risk person, ISEs should consider the following:
  - Whether there is a way to safety plan with the victim-survivor without directly disclosing the person of concern's information.
  - Whether the context of DFV may make it unsafe or inappropriate to share the information directly with the at-risk person.
  - Whether they have sought the views of the ISE that originally shared the information with them, to understand any concerns or sensitivities about sharing the information.
  - Whether the information is informed, accurate and not solely based on opinion.
- If an ISE is unsure about whether or how to share information with an at-risk person, they should seek secondary consultation in their own organisation, a specialist DFV service or the Information Sharing Coordinator.

Case Study 13: Determining what information is relevant to share

This is a continuation of Case Study 11. The Family Violence Safety Action Program (FVSAP) is authorised under the DFVISS to share information directly with Melissa if it is necessary for a protection purpose. Because of this, FVSAP informs Melissa that John has been attending her workplace and monitoring her family home, including the new car sometimes in her driveway.

In the example of John and Melissa, FVSAP knows that Melissa is unaware that John has been attending her workplace and residence to monitor her. FVSAP decides to share information with Melissa to support her ability to safety plan in response to John's stalking and monitoring. Without telling Melissa that her home is being monitored, FVSAP could not progress the safety planning needed to manage this risk.

FVSAP also discloses to Melissa that John has reported that his alcohol consumption has worsened, which is relevant to Melissa understanding the risk that John may pose to her.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Case Study 14: Deciding not to share information with an at-risk person directly

A specialist DFV service is an ISE under the DFVISS. They are working with Tania, who has come to them for support. Mark has been monitoring her phone, restricting her access to money and controlling who she can and cannot see. Mark is known to this ISE for perpetrating DFV against a former partner and the ISE is aware that Mark was previously convicted of family violence offences.

To facilitate effective safety planning, the ISE reaches out to ACT Corrective Services (another ISE) for further information about Mark's prior sentenced history. ACT Corrective Services share the facts of the prior sentenced matter which details his patterns of violence, as well as Mark's history of engagement under supervision of corrections during his 2-year non-custodial order. The DFV service working with Tania has made some gentle inquiries with her about Mark's prior relationship history, and it is clear the Tania either does not have knowledge about his prior relationship or that she is not sharing that information at this time.

The DFV service **does not** share the information about Mark's prior history with Tania. This is because they are of the opinion that sharing the information obtained from ACT Corrective Services might escalate DFV risk, either because Mark learns or suspects that this information has been given to Tania or because it may cause Tania to disengage from the service.

Instead of sharing the information with Tania directly, the practitioner uses the information they have received under the DFVISS to inform their risk management planning. Because the DFV service has broader context of Mark's behaviours, they can tailor their risk assessment and safety planning conversations to Mark's known patterns of violence.

Case Study 15: When sharing information with a victim-survivor could prejudice an investigation

This is a continuation of Case Study 6. The Family Violence Safety Action Program (FVSAP) is coordinating a response for Sarah and her child following a series of family violence incidents involving Sarah's ex-partner, George. Sarah has a current Family Violence Order (FVO) protecting herself and her child from George.

During an FVSAP meeting, ACT Policing shares information that George is allegedly involved in an organised crime network and is currently the subject of an active law enforcement investigation alongside the DFV matter. The information suggests George maintains contact with several associates who are also being investigated, but that the victim is not aware of their organised crime connections. The information has been provided to FVSAP for the purpose of their risk management planning.

During safety planning discussions, FVSAP identifies that Sarah may unknowingly encounter or seek assistance from some of George's associates because she is familiar with them through her previous relationship with George. An ISE member of FVSAP considers whether sharing information about George's organised crime involvement would assist Sarah to better understand and manage potential risks to her safety.

FVSAP consults with ACT Policing and carefully considers whether disclosure could have unintended consequences. They determine there are grounds to believe that sharing details about George's alleged organised crime involvement could prejudice the ongoing investigation. As a result, FVSAP collaboratively decides **not** to disclose the information to Sarah, but they take the information into account when planning and coordinating strategies to manage risk and support Sarah's safety.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

6. SHARING INFORMATION: AT-RISK AND CONNECTED PEOPLE

This Chapter provides guidance on how information sharing about **at-risk** and **connected people** works under the DFVISS. This includes information on consent requirements, as well as when to share without consent.

Sharing information about an at-risk person is not the primary way to assess and manage DFV risk, but it may form an important part of service provision and risk management practice. Wherever possible, this should occur with the consent and input of the victim-survivor, in accordance with DFVISS requirements.

ⓘ Remember

- An **at-risk person** is someone who has experienced, is experiencing, or may experience DFV. An at-risk person includes adults, children and young people.
- A **connected person** is a third party that has information that is relevant for a protection purpose. A connected person is a third party other than an at-risk person or person of concern. It could be a family member, friend, neighbour, colleague, or other third party.
- ISEs must not seek consent from a **person of concern** to share their information under any circumstances.

Key Points

- ISEs **need consent** to collect, use or disclose identifiable information about at-risk or connected people (see Chapter 6.1).
- **Consent** must be a freely given and informed decision. Best practice guidance and requirements on seeking consent is discussed in Chapter 8.
- ISEs need to first consider who is best placed to seek consent from an at-risk or connected person (see Chapter 6.2 and Figure 5). Services need to work together to streamline these processes in a safe and supportive way.
- ISEs must take **reasonable steps** to seek consent, if it is safe, reasonable and appropriate to do so (see Chapter 6.3).
- ISEs must provide at-risk and connected people **access to reasonable supports** to communicate their decision about consent (see Chapter 8.2).
- However, ISEs can share information about at-risk and connected people **without consent** in some situations, where it is necessary for the at-risk person's safety and protection (see Chapter 6.5).
- When you share information about **at-risk children or young people**, additional consent requirements apply (see Table 7 and Figure 7).
- Once you share information about an at-risk or connected person, ISEs have **notification requirements** under the DFVISS to inform people about how their information has been disclosed and used (see Chapter 6.6).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

6.1. Consent is required

Consent is a decision someone can make to give their permission for something to happen. For consent to be valid, a number of essential elements need to be present.

ISEs need consent to collect, use or disclose identifiable information about at-risk or connected people. A guiding principle of the DFVISS is to support the safety, dignity and agency of victim-survivors. Because of this, information about at-risk people and connected persons should generally only be shared with their consent. This recognises the important role victim-survivors have in keeping themselves safe, as they are experts in their own experience of DFV and the person engaging in tactics of violence and abuse.

Practice Guidance

- Consent is required if the information identifies the at-risk or connected person (see Chapter 6.4).
- ISEs need to also comply with the general consent thresholds and requirements summarised in Chapter 6.4.

6.2. Who should seek consent?

Not all ISEs need to obtain consent. ISEs should work together to streamline consent processes, so that victim-survivors do not experience unnecessary or repetitive contact with multiple agencies. Unnecessary or inappropriate contact can increase the system navigation burden on victim-survivors and place their safety at risk.

Not all ISEs will have an existing service relationship with a victim-survivor. Often, there is a **lead agency** coordinating support for the at-risk person. While the lead agency will usually share information about at-risk or connected people, other agencies may also raise a **risk concern** and want (or be asked) to share information they hold.

Practice Guidance

- **Lead agency coordination** is key to avoid multiple agencies contacting the victim-survivor unnecessarily.
- **Agencies raising a risk concern** should take responsibility for seeking consent (if safe, reasonable and appropriate) but involve the lead agency if one exists.
- In some circumstances, it may be more appropriate that a **different ISE** seeks consent.
- If consent has been given or an exception applies, other ISEs receiving the shared information are authorised to collect that information. However, victim-survivor information must not be on-shared to other ISEs, without the person's consent unless an exception applies (see Chapter 2.5).
- To understand who is best placed to seek consent, see Chapter 6.3.

Case Study 16: Risk concern agency working with a lead agency to seek consent

Megan's primary support is her child's school (Education). ACT Police request the school to provide Megan's pick-up and drop-off times so Police can investigate her ex-partner, who is monitoring her movements. While Police could contact Megan directly, the school discusses the request with Megan to obtain consent. This approach allowed Megan to maintain contact with her trusted support – the school – without needing direct engagement with Police.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

6.3. When should you seek consent?

Before you seek consent, you should make sure it is **safe, reasonable and appropriate** for your agency to do so. These considerations overlap.

In some circumstances, it may be more appropriate that a different ISE seeks consent, because it may be more safe, reasonable and appropriate for them. In other situations, information may need to be shared without consent if an exception applies.

Safe: Could contacting the person escalate risk?

- Risk to the person could be increased
- There is an immediate or serious risk
- The ISE does not know the victim-survivor's current circumstances, including *if* it is safe to contact them

Reasonable: Is it feasible, safe or practical to seek consent?

- You are not in a current service relationship with the person
- You are unable to make contact with the person

Appropriate: Could seeking consent be harmful, unsafe or unethical?

- It may be beyond the ISEs scope or expertise
- The person has expressed they do not want to have contact with a certain ISE

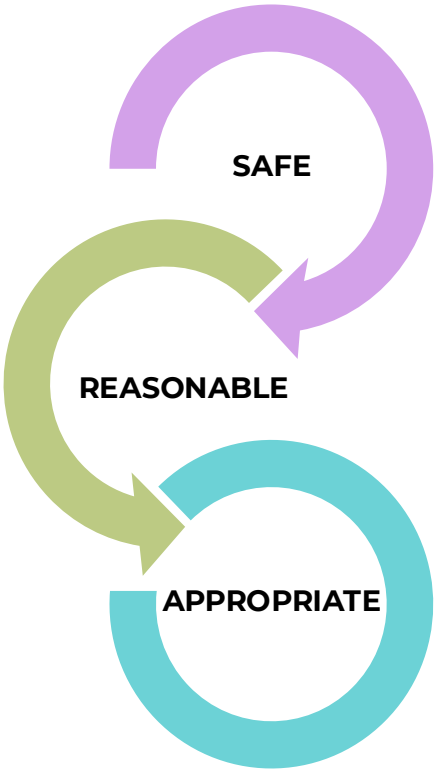


Figure 4: Seek consent when safe, reasonable and appropriate

Practice Guidance

- Consent should only be sought when **safe, reasonable, and appropriate** for your agency to do so.
- In some circumstances, it may be more appropriate that a **different ISE seeks consent** (see Chapter 6.2) or that information is shared **without consent** if an exception applies.
- These considerations will help ISEs determine appropriate steps for seeking consent. For example, if it is not safe for one ISE to make contact, that ISE may wish to engage another agency to seek consent, or wait to an appropriate time to engage with the at-risk person.
- By following the steps of the DFVISS, there will be times where an at-risk person's information cannot be shared. This reflects the purpose of the DFVISS in centring the agency and autonomy of those impacted by violence, and that sharing information without consent should be the exception – not the norm.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Should I seek consent?

Figure 5 describes the process a worker should undertake when considering what is appropriate in the context of their role, service provision and relationship with the victim-survivor about seeking consent to share their information.

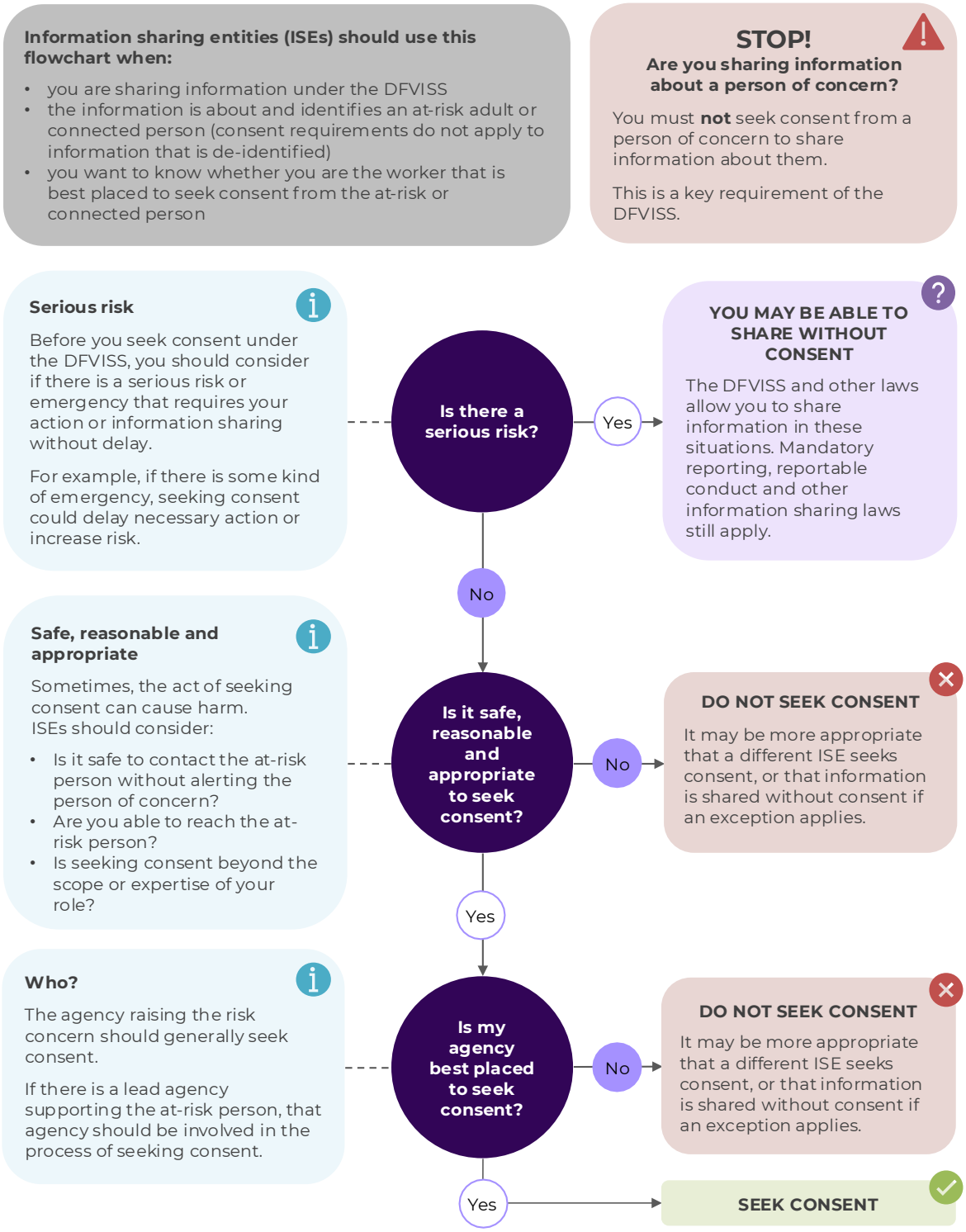


Figure 5: Flowchart - Should I seek consent?

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Case Study 17: Risk concern agency working with a lead agency to seek consent

Angelique is supported by Victim Support ACT (VSACT), which has established safe communication pathways with Angelique – they can only be contacted on a safe phone on Mondays between 2–5 pm. VSACT is the **lead agency**.

Canberra Health Services (CHS) recently treated Angelique and wants to share information about their admission with VSACT. This requires Angelique's consent. CHS does **not** have an ongoing service relationship with Angelique and does not know if contacting them is safe, but they know Angelique is working with a VSACT practitioner because this was disclosed during Angelique's recent admission.

To avoid unsafe or unnecessary contact, CHS asks VSACT to seek Angelique's consent to share information from the admission. VSACT uses its safe process to contact Angelique at the agreed time and explains CHS's request. Angelique consents and provides additional context about her visit. VSACT confirms consent to CHS, which then shares the relevant information to VSACT.

6.4. Requirements for consent

ISEs **need consent** to collect, use or disclose **identifiable information** about at-risk or connected people, unless an exception applies. When information is properly de-identified, consent requirements do not apply (see Chapter 2.3).

To understand how you can meet your consent obligations, refer to Figure 5 and Table 7. Figure 6 and Figure 7 help guide ISEs to practically apply the consent requirements for adults, children and young people.

Identifying versus deidentified information

Information is generally considered identifying if it could reasonably be used to identify, contact or locate the at-risk or connected person, either by itself or when put together with other pieces of information.

Sometimes, ISEs may decide to share information in a de-identified way. This may be for a variety of reasons, including:

- the at-risk person is feeling concerned about having their information shared with certain agencies, because of adverse experiences with certain system responses or other reasons.
- the ISE is seeking expert guidance or support through a secondary consultation from another ISE.
- sharing details or behavioural profiles with other ISEs to see if the patterns align with person using violence trends, without initially linking a specific victim-survivor's name to the inquiry.
- the ISE is seeking to request information about a person of concern.

Practice Guidance

- Consent is only valid when it is informed, voluntary, specific, current and the person has capacity to give consent (see Chapter 8.1).
- The DFVISS does not require that consent is given in writing. A person can communicate their decision about consent verbally, and an ISE should not unreasonably require a person to provide written consent. Record keeping requirements apply (see Chapter 7).
- ISEs may sometimes share information in a de-identified way, for a variety of reasons. If information is de-identified, that means it does not directly, or by inference, reveal information about a person that could cause another person to identify, recognise or know who the person is.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Table 7 summarises the consent requirements in the DVA Act, based on who the person is and their age.

DVA Act Requirement	Practice Guidance	At-risk: Adult	At-risk: Young Person	At-risk: Child	Connected person
AGE How old are they?	The person's age impacts requirements for consent.	18+ years	14 – 17 years	0 – 13 years	N/A – Refer to definition
CONSENT Is their consent required?	See Ch 6.4 See Figure 6 (adults), Figure 7 (children and young people)	Yes – from them[3]	Yes – from them or person with parental responsibility[4]	Yes – from person with parental responsibility	Yes – from them[3]
CAPACITY Do you need to assess decision making capacity?	Reasonable belief (see Ch 2.2) Capacity (see Ch 8.3)	No – unless they do not have sufficient capacity	No – unless they do not have sufficient capacity	No – a child is presumed to not have capacity to consent	No – unless they do not have sufficient capacity
PERSONAL FACTORS Are s 16(2) factors relevant?	See Ch 8.4	Yes	Yes[5]	Yes[5]	No – not required
REASONABLE STEPS Do you need to take reasonable steps?	See Ch 6.2, 6.3 Ch 8.1 See Figure 8	Yes – if safe to do so	Yes – if safe to do so	Yes – if safe to do so	Yes – if safe to do so
REASONABLE SUPPORTS Do you need to give access to supports?	See Ch 8.2	Yes	Yes	Yes	Yes

Table 7: Requirements for consent under the DVA Act

[3] If you reasonably believe an adult or connected person does not have decision-making capacity, you can seek consent from their authorised representative – if they are not the person of concern.

[4] If the young person does not have the decision-making ability to consent, the ISE must seek consent from the person with parental responsibility – if that person is not the person of concern.

[5] Even if a child or young person cannot consent to their information being shared, ISEs must take into account their age, maturity and decision-making ability when dealing with their information.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Sharing information about at-risk adults & connected people – Consent Requirements

Figure 6 describes how the consent requirements for at-risk adults and connected people should be applied when ISEs are seeking to share identifiable information about them.

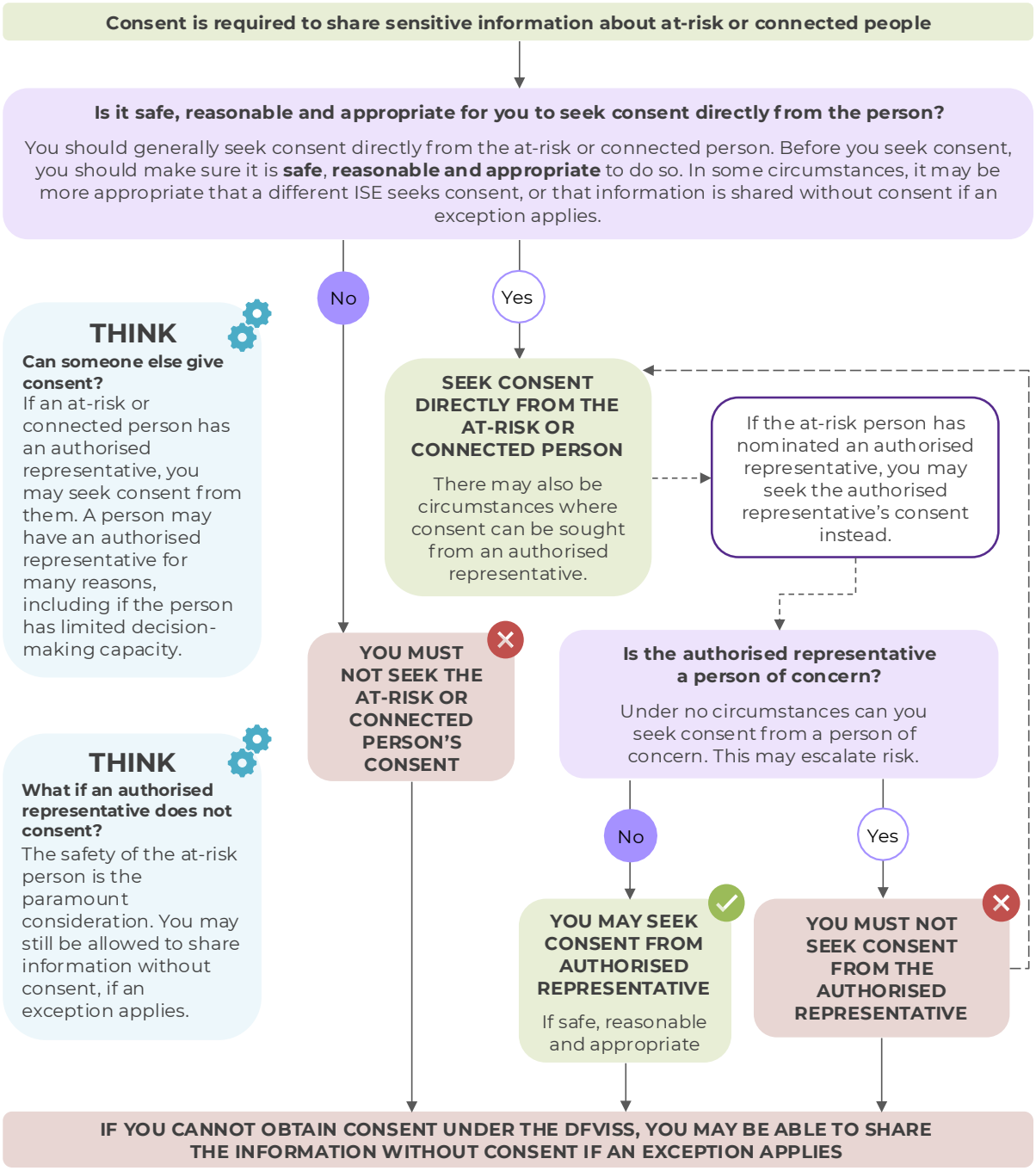


Figure 6: Flowchart - Sharing information about at-risk adults and connected people

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Sharing information about at-risk children and young people – Consent requirements

Figure 7 describes how the consent requirements for at-risk children and young people should be applied when ISEs are seeking to share identifiable information about them.

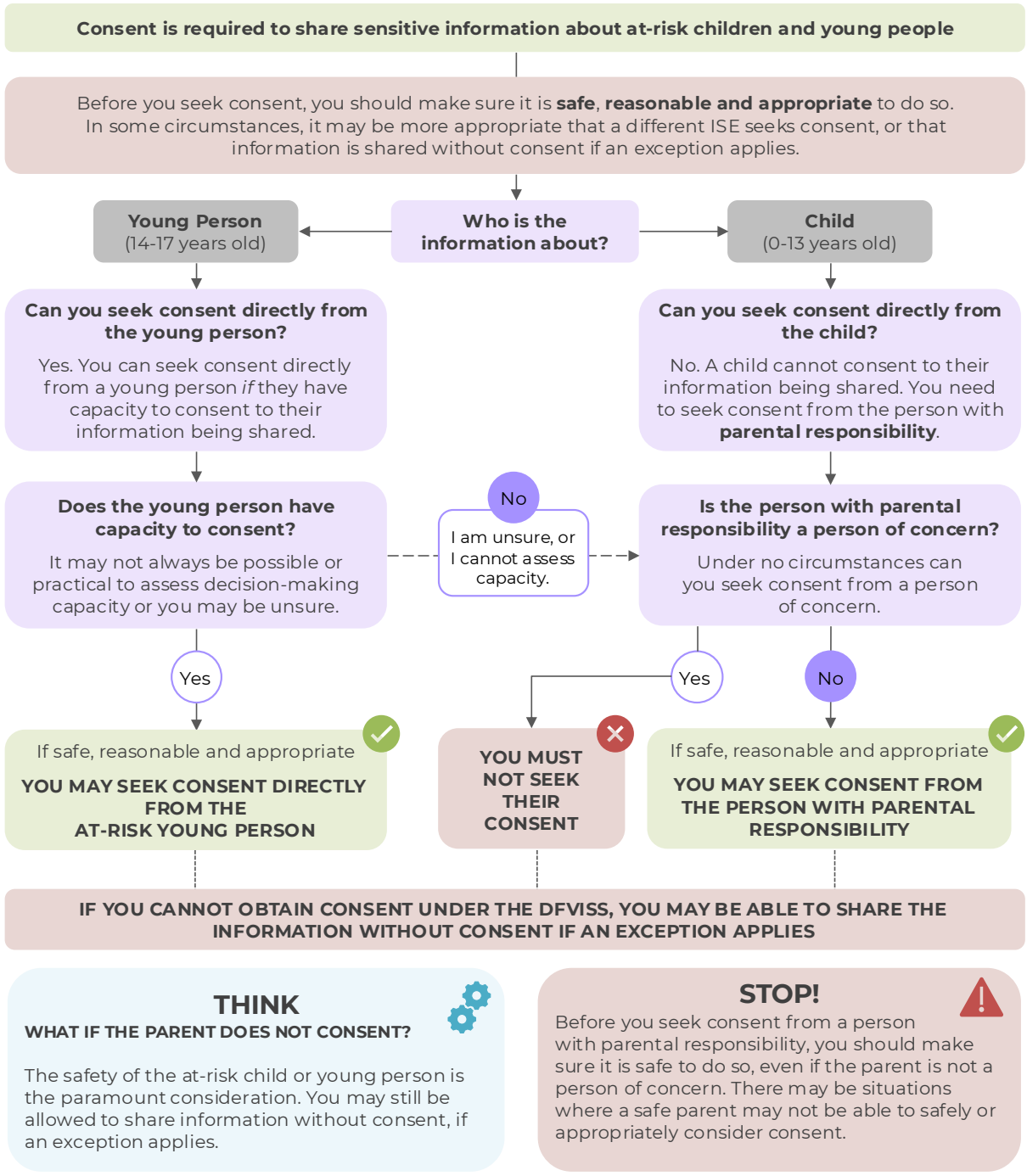


Figure 7: Flowchart - Sharing information about at-risk children and young people

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

6.5. Sharing without consent

There are **3 exceptions** where you can deal with information about an at-risk or connected person without their consent. In all scenarios**, dealing with the information must be necessary for the safety and protection of the at-risk person**. To understand how to apply the exceptions to consent in practice, see Figure 8.

ⓘ Remember

If you disclose information without consent, ISEs are still required to keep people informed about how their information has been used. However, you do not need to notify the person about the disclosure until it is safe or practical to do so (see Chapter 6.6).

Overarching threshold for consent exceptions

You must reasonably believe that dealing with the information is **necessary** for the **safety and protection of the at-risk person**.

Exception 1: Safety	Exception 2: Practicality	Exception 3: Serious risk
It is not safe to contact the person to seek their consent.	You cannot locate or contact the person, despite taking reasonable steps.	You may cause a serious risk to an at-risk or connected person if you fail to deal with the information.
This exception applies if you reasonably believe that seeking the person's consent **may cause a risk to life, health or safety** (theirs, or to another at-risk or connected person).	This exception applies if it is safe to seek consent, and you have been unable to reach the person despite taking reasonable steps to contact or locate them.	This exception applies if you reasonably believe that failing to deal with the information may cause a **serious risk** to the life, health or safety of the at-risk or connected person.

Table 8: Exceptions to sharing information without consent

Practice Guidance	Exception 1	Exception 2	Exception 3
Necessary for safety and protection (Ch 6.5)	✓	✓	✓
Not safe to contact (Ch 6.5)	✓	✗	✗
Risk (Ch 6.5)	✓	✗	✗
Serious risk (Ch 6.5)	✗	✗	✓
Reasonable steps to seek consent (Ch 8.1)	✗	✓	✗

Table 9: Practice guidance on how to practically apply the exception to consent

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Sharing information without consent (at-risk person)

Figure 8 outlines the scenarios when you can share information without consent of the at-risk person. This visual aid is designed to help ISEs operationalise the exceptions to consent to help meet DFVISS requirements.

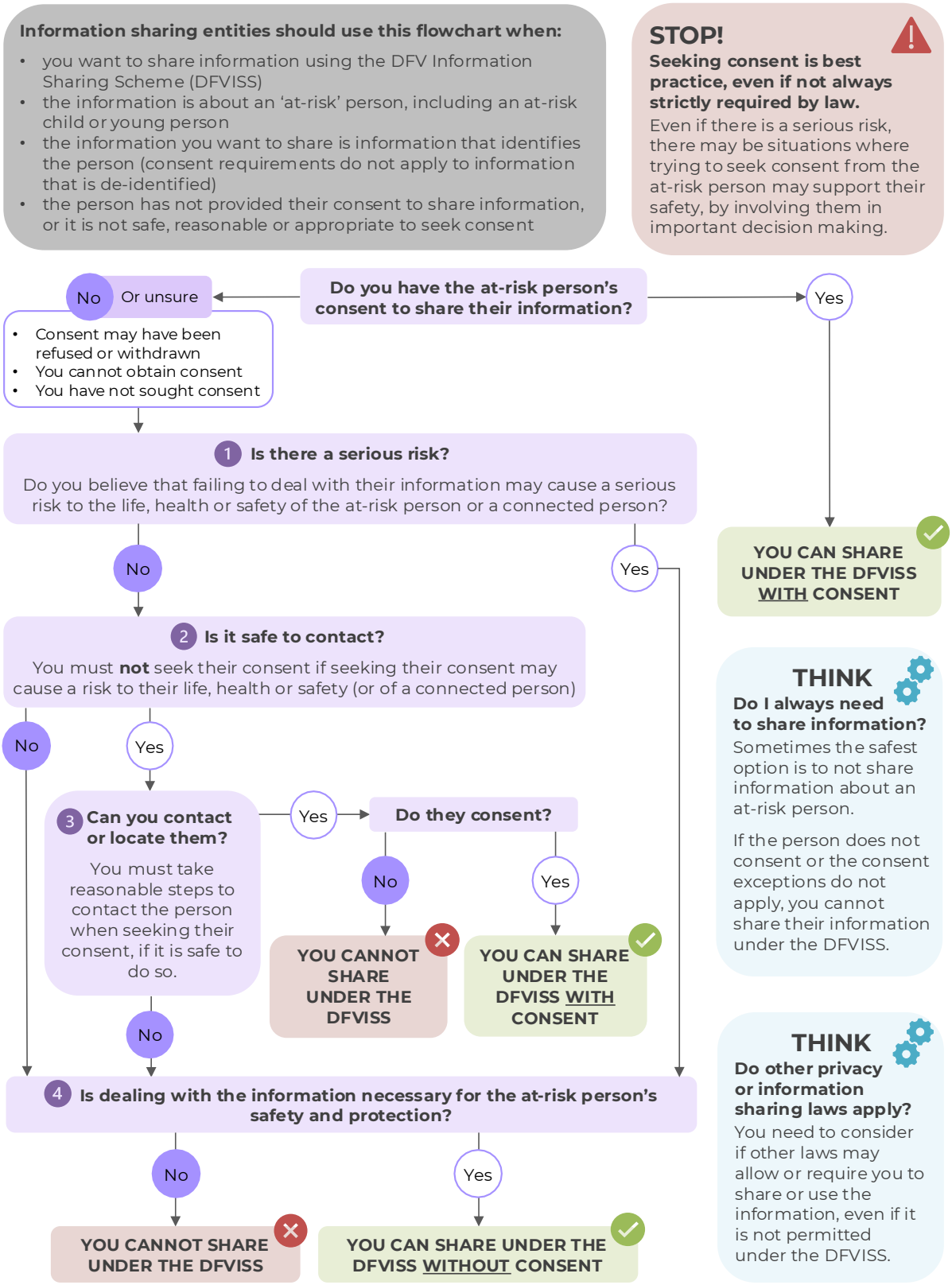


Figure 8: Flowchart - Sharing information without consent - At-risk person

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Necessary for safety and protection

Whenever sharing information without consent, ISEs must believe that it is **necessary** for the at-risk person's safety and protection. What is necessary will depend on the circumstances in each case. However, ISEs should consider:

- Will sharing or using the information **directly support** the safety and protection of an at-risk person?
- Is the information **related** to the safety, protection and wellbeing of the victim-survivor, a child in their care, or a person connected to them?
- Is the **intention** of sharing information to uphold or prevent a risk to the life, health or safety of the victim-survivor?
- Can you **delay** dealing with the information to first seek consent, provided it is safe to do so?
- Will delaying the disclosure of information **risk the safety** of the victim-survivor?
- Could dealing with the information without consent **increase** risk to the at-risk person?
- Have you collaborated with a lead agency working with the at-risk person to understand how the risk profile may change if you share without consent?

Practice Guidance

- What is necessary is based on a reasonable belief. This does not require that you are certain about an outcome (see Chapter 2.2).
- The severity and likelihood of risk, the nature of harm, and the at-risk person's experience of violence is relevant to understanding when sharing information may be necessary.
- ISEs should also consider the at-risk person's views on risk and service intervention, where known from prior engagement.
- ISEs should consider how risk of harm to people, property and pets might inform an assessment of safety and protection.

'Not safe' to contact

The following non-exhaustive list provides examples of when it may not be safe to contact someone:

- The victim-survivor lives with the person using violence
- The person using violence has a history of coercing information from the victim-survivor, including who they speak to
- The person using violence may be monitoring the victim-survivor's phone
- There is a history of stalking or technology facilitated abuse

Practice Guidance

- If contacting a person to seek their consent may cause a risk to their life, health or safety (or to another at-risk or connected person), it is not safe to contact them.
- ISEs should focus on what the outcome of seeking consent would be. For example, if seeking the at-risk or connected person's consent could alert the person of concern that services are involved, this could escalate the risk of DFV harm to a victim-survivor.
- If an ISE believes it is not safe to contact the at-risk person, the ISE should communicate this to other relevant ISEs who are engaging with the at-risk person.
- In some circumstances, it may be safer and more appropriate that a **different ISE** seeks consent. See practice guidance in Chapter 6.2.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

May cause a 'risk' or a 'serious risk'

A **risk** is a potential for harm. ISEs must rely on the **ACT RAMF** to assess for risk. For example, it might be reasonable to believe seeking consent would cause a risk to the person in the following situations:

- Where the at-risk person lives with the person of concern.
- Where the person of concern has a history of extracting information from the victim-survivor about what they have done or who they have talked to.
- Where the person of concern is monitoring or controlling the at-risk person, including through monitoring their electronic devices or stalking them.

A **serious risk** is one where the potential for harm is severe and/or more likely to occur. It is a higher threshold, because if a person has refused consent or consent cannot be obtained, there must be a compelling reason to deal with their information. The circumstances may be urgent, but not all examples of serious risk will always be urgent or immediate.

For example, it might be reasonable to believe someone is at serious risk of harm in the following situations:

- Experiencing or witnessing multiple incidents of DFV (cumulative harm) may constitute a serious risk, especially for children and young people.
- Situations which involve evidence-based risk factors for serious harm or lethality (see the ACT RAMF).
- A victim-survivor's reported level of fear.
- Other factors such as severity, likelihood, timing and nature of the harm.

This risk to life, health or safety does not need be imminent. It is sufficient to establish a threat is serious and that disclosure is necessary to reduce or prevent that threat.

Practice Guidance

- A risk refers to a potential for harm. A serious risk is where the potential for harm is severe and/or more likely to occur. If relevant, ISEs should rely on the **ACT RAMF** to help their consideration of what a serious risk may include.
- It is not a requirement that a risk is imminent, even for a serious risk.
- ISEs should refer to the considerations explored in this section of the Ministerial Protocol.
- ISEs also need to consider the potential *outcome* of seeking consent, and how this might change the risk profile. While this may be informed by the ACT RAMF, the presence or not of ACT RAMF risk factors will not necessarily help ISEs decide if there is a risk or serious risk in relation to seeking consent.
- An ISE does not require proof that the harm or identified risk will occur. It is a credible risk based on the circumstances known to the practitioner at the time.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Case Study 18: Not safe to contact an at-risk person – potential for risk

Selina, a 17-year-old high school student, lives with her parents, Stephanie and Joe. Selina has been supported by a specialist DFSV provider to report Joe for a long history of sexual abuse. Joe is unaware of the report. Selina told Police that Joe monitors her phone and location, and she fears being caught. He has threatened that her 'life won't be worth living' if she tells anyone about the abuse.

Police are preparing to charge Joe and inform both Selina's school and the DFSV provider of their plan to lay charges while Joe is at home and Selina is at school. They are concerned that Joe's reaction to the arrest will place Selina at risk, and may be upsetting for her. The school advises that Selina has been unwell and absent all week, confirmed by her mother Stephanie. Concerned that Police might arrest Joe without realising Stephanie is home, the school decides it is necessary to share this information with Police without seeking Selina's consent, given Joe's history of controlling and threatening behaviour.

Case Study 19: Serious risk

Later that week, Selina's friend tells a teacher that Selina messaged her using a different social media account, saying Joe had found out that she "told someone about him" and that she was scared he might hurt her. The friend shows the teacher the message, which ends abruptly, and says Selina hasn't responded since.

The school believes that her life or safety may now be at serious risk. In these circumstances, the school decides it is necessary to disclose Selina's personal information – including her recent communication details – to Police so they can urgently check on her welfare.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

6.6. Notification requirements

Once information has been shared under the DFVISS, ISEs must notify at-risk and connected people about the disclosure and use of their information, except in certain situations. This supports keeping at-risk and connected people informed about how their information is being dealt with, so that information sharing can occur in a safer and more collaborative way that builds trust with those impacted by violence.

ⓘ Remember

Notification requirements only apply to dealing with information about at-risk and connected persons. **ISEs must not notify or tell a person of concern** that information was dealt with under the DFVISS (see Chapter 5.1 on specific guidance on safely applying this requirement).

Table 10 summarises the DVA Act notification requirements, explaining when ISEs need to notify at-risk and connected people about how their information has been dealt with under the DFVISS.

Activity under the DFVISS: You have...	**Notification requirement:** You must...	**Content of notification:** The notification must include...
Disclosed information for a protection purpose Section 16AQ	Tell the at-risk or connected person about the disclosure.	• The name of the ISE that received the information; • The date of disclosure; • The nature of information disclosed; and • Any outcomes of disclosure.
Proposed action for a protection purpose Section 16AR	Tell the at-risk or connected person about the proposed action and risk.	• The proposed action; and • The risk the ISE believes the action may cause.
Disclosed or used information for a secondary purpose Section 16AS	Tell the at-risk or connected person about the disclosure or use.	• The ISE that received or used the information; • The date of disclosure or use; • The nature of information disclosed or used; and • Any outcomes of disclosure.

Table 10: Notification requirements under the DVA Act

Protocol Requirement

- **How to inform the person:** An ISE must not inform a person in writing if it would cause a risk to the life, health or safety of an at-risk person or connected person.
- **Timeframe:** An ISE must notify the person as soon as reasonably practicable.

Practice Guidance

- Consider whether it is safe to notify the person (see exceptions at Figure 8 and Chapter 6.6).
- Remember that ISEs have record keeping obligations about notification (see Chapter 7).
- ISEs should note that other laws may restrict what they can tell people about how certain information has been shared. See for example restrictions on sharing information about who makes a mandatory report under the *Children and Young People Act 2008.*

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Exceptions to notifying an at-risk or connected person

Table 11 summarises the circumstances and exceptions for when notification requirements do not apply.

Exceptions You do not need to notify the person if…	**Disclosure (protection purpose)** Section 16AQ	**Proposed action[6] (protection purpose)** Section 16AR	**Disclosure or use (secondary purpose)** Section 16AS	**Practice Guidance** ISEs should consider…
The person does not want to be told[7]	✓	✗	✓	• Seeking the person's views on notification when obtaining consent
Another entity told the person	✓	✓	✓	• Which ISE is best placed to tell the person – Ch 6.3
It is not practicable to tell the person	✓	✓	✓	• If it is not feasible to notify them, given the means, circumstances or resources – Ch 6.3
It is not safe to tell the person[8]	✓	✓	✓	• Belief – Ch 2.2 • 'Not safe' – Ch 6.5 • 'Risk' – Ch 6.5
The person consented to the disclosure	✗	✗	✓	• If the person consented to secondary disclosure or use, ISEs do not need to notify the person.

Table 11: Matrix of what exceptions apply to each notification requirement

Table 11 Notes:

✓ Exception applies – You do not need to notify the person.
✗ Exception does not apply – You still need to notify the person.

Protocol Requirement

- If not safe to tell the person, the ISE must consider notifying them when it becomes safe to do so.

Practice Guidance

[6] This exception only applies if an ISE proposes to take an action, and the ISE reasonably believes the proposed action may cause a risk to the life, health or safety of the person (see Chapter 6.3).

[7] The person must have told you this in writing.

[8] If you disclosed or used their information without consent because of the same exception to consent (e.g. risk to life, health or safety), you do not need to notify the person until it is safe to do so.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

7. RECORD KEEPING

This Chapter outlines practical guidance on how to make, store, keep, correct and destroy records under the Domestic and Family Violence Information Sharing Scheme (DFVISS).

Key Points

- ISEs, where relevant, will need to continue to meet any existing record keeping and privacy requirements under relevant records and privacy legislation. This will not apply to all ISEs, as some non-government organisations are not captured by Territory or Commonwealth record keeping and privacy laws.
- However, all ISEs must maintain accurate records of information, actions and decisions made or dealt with under Part 3 of the DVA Act (see Chapter 7.1).
- Other usual record keeping requirements described in this Chapter are about keeping accurate records, maintaining the security of personal information, disposing of records appropriately, and correcting inaccurate or incomplete records.
- Chapter 7.2 contains the minimum suggestions of what information should be recorded under the DFVISS.
- For records held by some ISEs, information may be able to be accessed under territory records or freedom of information laws, subject to certain exceptions (see Chapter 7.5).
- Good record keeping practices will make it easier for an ISE to establish that they have dealt with information appropriately and therefore entitled to the protections under the DVA Act (see Chapter 10).
- All ISEs should update their own internal policies and procedures to reflect their powers and obligations to collect, use and disclose information under the DFVISS.
- ISEs have additional special record obligations created under this Ministerial Protocol, to support their ability to meet their obligations under the DFVISS. This relates to ISEs needing to use information tags on their record keeping systems to track key pieces of information (see Chapter 7.7).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

7.1. Requirement to keep records

Accurate records will support ISEs to be able to meet and demonstrate their compliance with obligations under the DFVISS, as well as ensuring information is shared, used and disclosed in a safe and appropriate way. The nature and extent of record keeping and management obligations will depend on whether an ISE is covered by Territory or Commonwealth privacy and records management laws.

Protocol Requirement

- All ISEs must maintain accurate records of information, actions and decisions made or dealt with under the DFVISS. This includes the collection, use or disclosure of information.
- ISEs that are not covered by relevant Territory or Commonwealth laws must still make and keep full and accurate records of their activities under the DFVISS.

Practice Guidance

- If an ISE is covered by any relevant privacy or record keeping laws, record keeping practices under the DFVISS must align with relevant legislation.
- All ISEs should ensure their policies and procedures are updated to reflect their obligations to collect, use and disclose information under the DFVISS.
- Record keeping practices will likely vary from agency to agency, due to the different operational and service settings of ISEs. Record keeping practices may include saving email correspondence and file noting conversations or decisions.

7.2. What should be recorded?

There are 5 general record keeping checkpoints ISEs can encounter across the DFVISS. Chapter 7.2 provides guidance on what information should generally be recorded under the DFVISS, and this is summarised by **Figure 9**.

Sharing or Requesting Information	• ISEs should record details of **information sharing requests** and **responses,** including how **consent** is dealt with under the DFVISS. • ISEs have special obligations to 'tag' information they receive and share. These **information tag** requirements are detailed in Chapter 7.7.
Refusing to share	• All **refusals to requests for information sharing**, including the request and reason for refusal, should be recorded.
Actions taken	• When ISEs use information received under the DFVISS, they should record the **actions taken to prevent, respond or manage DFV risk**, arising from the information recieved.
Informing people	• When ISEs share or use information about an at-risk or connected person, they should record **whether they told the person about the disclosure or use** of their information.
Complaints	• ISEs should keep a record of complaints they recieve under the DFVISS.

Figure 9: Summary of the five record keeping checkpoints across the DFVISS

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Sharing information

ISEs should record details of information sharing requests and responses under the DFVISS.

Practice Guidance		
Information tags	• ISEs have special record keeping obligations to 'tag' information they receive and share.	• **Special record obligations** – Ch 7.7
Information sharing requests, responses and activities	ISEs should record their activities under the DFVISS, including: • Any requests they make or receive • Information shared with them (either directly or through multiagency forums for information sharing) • What information they share with others (including another ISE or at-risk person) ISEs should **record the details** of these information sharing requests, responses and activities, including: • who requested and shared the information • what information was shared and for what purpose under the DFVISS • when the request was made or information was shared	• How to **request and share** information – Ch 2.5, Figure 2, Figure 3 • Consideration of **personal factors** (where relevant) – Ch 8.4 • **Why you can share (purpose) –** Ch 2.2
When sharing about at-risk or connected people	ISEs should also record: • If consent was given, a **record of consent** (written or verbal) – A record of consent should include who consented, to what, the date, and if reasonable supports were provided (if applicable), including if consent is later withdrawn. • If information is shared without consent: – Why consent was not obtained, sought or refused (i.e. what was the reason the ISE relied on to share information without consent)	• **Consent requirements** – Ch 6.4, Figure 6, Figure 7 • **Consent exceptions** – Ch 6.5, Figure 8 • **Capacity** – Ch 8.3

Table 12: Practice guidance for record keeping when sharing information

Refusing to share information

Practice Guidance	
An ISE may **refuse a request to share information** if a relevant ground under the DVA Act applies (see Chapter 2.6). Where an ISE refuses a request to disclose information about any person, it should record: • Details of the request to share information; • Relevant ground for refusing to share; and • Record of telling the Information Sharing Coordinator about the refusal.	• **ISC** – Ch 4.3

Table 13: Practice guidance for record keeping when refusing to share information

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Actions taken under the DFVISS

ISEs may use information to **take action to prevent, respond or manage domestic and family violence risk.** Actions can include things other than information disclosures (see Chapter 2.5).

Practice Guidance

Where an ISE takes an action to prevent or reduce the risk of DFV, or otherwise does something to manage DFV risk in response to information that has been shared, the ISE should record: • Any action or decision relevant to preventing, reducing or managing DFV risk.	• Guidance of **taking actions** – Ch 2.5

Table 14: Practice guidance for record keeping when taking an action under the DFVISS

Informing people about disclosure, use and actions

Once information has been shared under the DFVISS, ISEs must generally **notify at-risk and connected people** about the disclosure and use of their information (see Chapter 6.4).

Practice Guidance

Protection purpose	ISEs should record: • If the person was told about the disclosure and/or action; and • If the person was not told, what was the reason the ISE relied on to not inform the person.	• **Protection purpose** – Ch 2.2 • **Notification requirements** – Ch 6.6
Secondary purpose	ISEs should record: • Whether the person was told about the disclosure or use; • If the person was not told, what was the reason the ISE relied on to not inform the person; and • How and what the ISE told the Information Sharing Coordinator about the disclosure or use.	• **Secondary purpose** – Ch 2.5 • **Notification requirements** – Ch 6.6 • **ISC** – Ch 4.3

Table 15: Practice guidance for record keeping when informing people about information use or disclosure

Complaints

Practice Guidance

If a complaint is made to an ISE about the exercise of their functions under the DFVISS, it should record: • The date of complaint; • The details of complaint; • The actions taken to resolve complaint; • The time taken to resolve; and • Any further actions taken (if relevant).	• **Complaint processes** – Ch 10

Table 16: Practice guidance for record keeping when an ISE receives a complaint

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

7.3. How should ISEs store information?

Safe and secure record management supports victim-survivor safety and increases confidence and collaboration between ISEs by managing the risk of intentional and unintentional privacy breaches.

ⓘ Remember

A security breach under the DFVISS may constitute an offence and attract civil liability. ISEs who take reasonable steps to manage the risk of security breaches will support safer information sharing and make it easier to establish they are entitled to the offence exceptions and liability protections under the DVA Act.

ISEs must take reasonable steps to protect personal information they hold from misuse, interference or loss, and unauthorised access, modification or disclosure. In determining if a step is 'reasonable', ISEs must consider the potential impact of a possible security breach of the information. The greater the impact of a security breach, the greater the need to take steps to protect that information.

Possible impacts from security breaches can increase domestic and family violence risk. For example:

- A person of concern could escalate their violence towards an at-risk person
- A person of concern could weaponise information they learn about the at-risk person and/or other family members, including children, to further control or isolate them
- A person of concern could make more efforts to disguise or hide their violence to prevent detection and intervention by services
- A breach of an at-risk person's privacy could cause them to lose trust in certain services, and impact their help-seeking behaviours

Reasonable steps an ISE can take may include some of the following strategies or steps:

- **governance, culture and training** (e.g. information security training to support understanding of obligations)
- **internal practices, procedures and systems** (e.g. standard procedures outlining security measures to mitigate risks and threats to personal information breaches)
- **ICT security** (e.g. software, network and email security, backing up, encryption)
- **access security** (e.g. establishing security levels to limit access to necessary staff, using individual password protection for computer and database access)
- **third party providers** (e.g. including cloud computing)
- **data breaches** (e.g. preventing and responding to them)
- **physical security** (e.g. locking filing cabinets and unattended storage areas

Protocol Requirement

- All ISEs must take reasonable steps to protect personal information they hold from misuse, interference or loss, and unauthorised access, modification or disclosure. In determining if a particular step is 'reasonable', ISEs must consider the potential impact of a possible security breach of the information.

Practice Guidance

- If the impact of a possible security breach could escalate DFV risk, ISEs will usually have a greater responsibility to take reasonable steps to protect that information.
- ISEs working directly with a person of concern (or both a person of concern and at-risk or connected person), should consider keeping separate files to manage the risks of unauthorised disclosure.
- ISEs may need to separate information from a person's file and use a flag to indicate the presence of this information. This includes risk identification and assessment tools, and safety planning.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

7.4. How should information be destroyed?

For ISEs that are subject to the *Territory Records Act 2002* (the Territory Records Act), information that is dealt with under the DFVISS are territory records. This means that territory records can only be destroyed in accordance with an approved schedule providing for the disposal of records. If an approved schedule for record disposal is in force, this can be accessed through the ACT Legislation Register. Entities subject to the Territory Records Act are defined in section 7 of that law.

ISEs that are not covered by territory records legislation do not have records destruction requirements or obligations under the *Territory Records Act 2002*. Instead, these ISEs should retain records for as long as they deem it is necessary. When information is no longer needed for a protection purpose, those ISEs may dispose of those records. These ISEs may otherwise choose to implement the principles outlined in the Standard on Records and Information Governance released under the *Territory Records Act 2002*. Some ISEs may be subject to other laws about records disposal, including Commonwealth legislation.

7.5. Accessing information

Under Territory and Commonwealth privacy laws, **people generally have a right to access and correct their personal and health information** that is held by an organisation. Rights of access to information are not absolute. Limitations and exemptions apply under various laws.

Territory records legislation

Territory agencies that hold DFVISS records are subject to the *Territory Records Act 2002*, including in relation to public access. Note that public access under the Territory Records Act only applies to records that are more than 20 years old. However, a declaration can be made under section 28 of the Territory Records Act to exempt territory records from public access. The Territory Records Office can assist ISEs that are subject to the Act to apply for exemptions from the public access arrangements. Please visit the Territory Records Office website for up-to-date information on whether public access provisions apply to the DFVISS.

Freedom of information legislation

Information an ISE holds only because of Part 3 of the DVA Act cannot be disclosed under the *Freedom of Information Act 2016* (the FOI Act). ISEs must refuse freedom of information requests for information they hold, only because it was disclosed to them under Part 3. This does not impact the application of the FOI Act to information which an ISE receives, holds or generates outside of Part 3. In practice, members of the public will need to apply to the original entity that generated the information. For example, if ISE 1 shared information with ISE 2, a member of the public can only seek that information from ISE 1. ISE 2 is not allowed to disclose information under freedom of information laws, because they only hold the information because of the DFVISS.

Practice Guidance

- The FOI Act does not apply to information an ISE holds only because of information sharing under Part 3 of the DVA Act.
- Open access under the *Territory Records Act 2002* may not apply to Part 3 of the DVA Act if an exemption for the DFVISS is in force.
- ISEs should update internal policies, protocols and communications about requests to access information, in line with the DFVISS and other applicable laws.
- ISEs should tag the source of information they share and/or receive under the DFVISS (see Chapter 7.2 and 7.7). This will help ISEs manage their access obligations.
- ISEs should ensure that, when providing a person access to information about themselves (where permitted), there is no unreasonable impact on the privacy of others.
- ISEs should be especially careful about the impact on victim-survivor safety, if a person of concern is seeking access to information.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

7.6. Correcting information

All ISEs have a responsibility to ensure their records are accurate. Incorrect information may put a victim-survivor at risk or lead to a victim-survivor being misidentified as a person using violence (see Chapter 5.3). Correcting inaccurate information may also assist in rebuilding the relationship between a client and their support service.

Protocol Requirement

If an ISE becomes aware that information they hold about any person is incorrect, or a person requests their information is corrected, the ISE must take reasonable steps to:

- **correct** information on their records, to ensure that the information is accurate, up-to-date, complete, relevant and not misleading.
- **notify any entity** that has received the incorrect information, unless it is impracticable or unlawful to do so.
- **notify the at-risk person** about the use of incorrect information, if it is safe, reasonable and appropriate to do so (see Chapter 6.2 and 6.3).

Practice Guidance

- Information may be considered 'incorrect' if the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. For example, records must be updated if a person withdraws previously given consent.
- ISEs should correct information as soon as reasonably practicable once they are aware the information is incorrect.
- Any correction should be prominent on the person's file.
- Incorrect information includes where misidentification has occurred (see Chapter 5.3).

7.7. Special record obligations

When information is shared under the DFVISS, ISEs will need to use 'information tags' on their record keeping systems to track key pieces of information.

The source of information

The DFVISS only applies to information that is shared or received under Part 3 of the DVA Act. If an ISE receives or holds information because of another law, the DFVISS requirements do not automatically apply. **ISEs therefore need to keep track of the source of information they hold.** For example, whether information they have received from another entity was given to them because of the operation of Part 3 of the DVA Act, or another law. This will support ISEs to manage the following requirements under the DFVISS:

- If information has been received under the DFVISS, ISEs are limited in how they can use or share that information under other laws for a secondary purpose (see Chapter 2.5).
- If an ISE holds information only because of the DFVISS, the *Freedom of Information Act 2016* does not apply to that information (see Chapter 7.5).
- Offences and liability provisions, including protections for workers, only apply to information that has been shared under Part 3 of the DVA Act (see Chapter 10).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Protocol Requirement

- ISEs must record when they are relying on Part 3 of the DVA Act to share information, or when they have received information under Part 3.

Practice Guidance

- This may be achieved by clearly marking internal file notes or emails relating to information sharing under the DFVISS, that the information was shared because of Part 3 of the DVA Act.
- Multiagency information sharing forums may wish to expressly consider and identify what laws they rely on to share information, to maintain consistency and clarity in what obligations apply.
- ISEs may also record the original source of the information, if they are aware.

Use and derivative use immunity

Some ISEs may have powers to **compel information** under other laws, or they may receive information from an organisation that has compelled the information. Compelled information may attract a **use or derivative use immunity**. This immunity can prevent compelled information from being used against a person in a legal proceeding, including any evidence or information obtained as a result of the compelled information.

Importantly, **sharing compelled information is not prohibited under the DFVISS, provided that the requirements for the DFVISS are met.** Generally organisations with an investigative or prosecutorial function are those responsible for understanding the implications of using and relying on compelled information. There are few ISEs that separately hold powers to compel information under their laws on pain of criminal penalty. However, those organisations need to know when information has been compelled. To ensure that compelled information is shared and used appropriately under, ISEs need to record when they receive or share information that has been compelled.

ISEs should note that information which has been required to be shared under the DFVISS, through a decision made by the Information Sharing Coordinator, is not 'compelled information' for the purpose of use and derivative use immunity.

Protocol Requirement

- If an ISE receives compelled information under the DFVISS, it must record that fact.
- If an ISE shares compelled information under the DFVISS, it must ensure the receiving ISE is aware that the information originates from a compelled source.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

8. GOOD PRACTICES IN INFORMATION SHARING

This Chapter outlines practical considerations for ISEs when obtaining consent, including reasonable supports, reasonable steps to contact an at-risk or connected person and assessing their capacity to make decisions about consent. This Chapter also describes key practice considerations for working with priority cohorts, as informed by the ACT RAMF.

Key points

- Consent is a person's decision to give permission for something to happen or agreeing to do something. ISEs who share identifiable information about at-risk or connected people must do so with their consent, unless an exception applies (see Chapter 6.5). This is a fundamental safeguard of the DFVISS.
- Consent is only valid if it is informed, voluntary, specific, current and the person has capacity to give their permission (see Chapter 8.1).
- ISEs need to take reasonable, genuine attempts to seek a person's consent. See Chapter 8.1 to understand what reasonable steps might involve, on a case-by-case basis.
- ISEs must give people access to reasonable supports, so that the person can communicate their decision about consent (see Chapter 8.2).
- There are times when an ISE may need to assess the decision-making capacity of an adult or young person. See Chapter 8.3 for general guidance on assessing capacity.
- Part 3 of the DVA Act requires ISEs to consider personal factors about certain at-risk people when dealing with their information. These factors are important considerations for ISEs to tailor their service and information sharing practices to ensure they are responsive to the distinct needs of key cohorts (see Chapter 8.4).
- If consent is not given or it is withdrawn, ISEs may still be able to share the person's information is exceptional circumstances. This includes scenarios where there is a serious risk and sharing the information is necessary for the at-risk person's safety and protection (see Chapter 6.5).

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

8.1. Obtaining consent

Consent involves someone giving permission for something to happen, or agreeing to do something, after being provided all relevant information to make an informed decision.

Whenever seeking consent in accordance with the requirements and guidance in Chapter 6, ISEs must ensure that consent is validly given.

Consent will only be valid if it meets the 5 essential best practice elements: that is, consent must be **informed**, **voluntary** (i.e., freely given), **specific**, **current** and the person must have **capacity** to give consent. This reflects a best practice approach to seeking consent, including for victim-survivors of DFV.

ⓘ Remember

- Any consent under the DFVISS must be informed, voluntary, specific, current and the person must have capacity to give consent.
- A person can communicate their decision about consent verbally or in writing, and an ISE must not unreasonably require a person to provide written consent (see Chapter 6.4). Record keeping requirements apply (see Chapter 7).
- ISEs are required to keep accurate records. This includes the responsibility to correct information that is considered 'inaccurate' or 'out-of-date'. An at-risk or connected person may withdraw consent at any time, either verbally or in writing. ISEs should consider their record keeping obligations in this scenario (see Chapter 7).
- Information may be shared without consent, such as when consent has been withdrawn or refused, if a valid exception applies (see Chapter 6.5).

Take reasonable steps to seek consent

The DVA Act requires ISEs to take reasonable steps to locate or contact the at-risk person when safe to do so, before dealing with their information without consent (see Chapter 6.5).

Taking 'reasonable steps' means an ISE has made a **genuine attempt** to contact or locate the at-risk person, to the extent that a reasonable person in their circumstances would do so.

Practice Guidance

Depending on the circumstances of the situation and the particular at-risk person, reasonable steps to seek consent may involve:

- Using a known safe communication mode to contact the person (including phone, email, in person, through a support person)
- Giving the victim-survivor reasonable time to respond
- Adopting a proactive outreach approach where appropriate, such as:
  - follow up contact,
  - visiting victim-survivors at a safe place (only if appropriate and within the scope of a worker's service provision),
  - providing flexibility around the time-of-day communications take place, and
  - communicating in adaptive ways to meet the person's needs.
- It is important that attempts to contact the victim-survivor do not escalate the risk of harm.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Five essential elements of consent

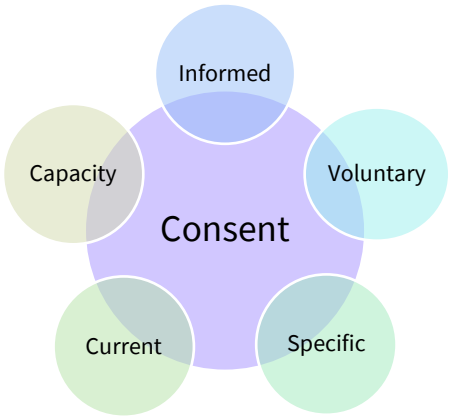


Table 17 outlines supporting practice guidance for ISEs in seeking consent, according to the 5 essential elements: **informed**, **voluntary**, **specific**, **current** and **capacity**. If these elements are not met, any "consent" given is not valid and may impact safe information sharing.

These considerations often overlap with one another, and ISEs should rely on the practice guidance to support their general policies and procedures when seeking consent from service users. Ultimately, consent practices are about centring the agency of victim-survivors and those impacted by violence, and empowering their decision-making about matters that affect their lives.

Figure 10: Five elements of consent

Consent Elements	Practice Guidance
Consent must be fully **informed**	This means the person has full knowledge of relevant facts and understands what they are consenting to. ISEs can support informed consent by: • Explaining what information will be collected, used or disclosed • Explaining how and why their information may be shared • Providing this information in accessible formats • Informing the at-risk person that they will be notified about the use of their information when the Scheme requires (see Chapter 6.6).
A person must have **capacity** to communicate their decision about consent	• A person's decision-making capacity is linked to the considerations about informed consent. • For information on assessing capacity, see Chapter 8.3. • For guidance on providing access to reasonable supports, see Chapter 8.2.
Consent must be **voluntary**	This means the person must be able to freely make a decision about consent, with undue pressure, influence, threat or coercion. • ISEs should consider the unique pressures and concerns the person might be facing. • ISEs should conduct discussions about consent away from people who may influence the decision. • For guidance on working with priority cohorts, see Chapter 8.4.
Consent must be **specific** and **current**	Consent must relate to the specific circumstances and purpose for sharing information. Consent does not continue indefinitely. • ISEs should not seek a broader consent than is necessary. • When seeking consent, ISEs should discuss how long consent will be valid for and the circumstances which might impact the validity of consent, including if the consent is limited for disclosure to certain ISEs. • If circumstances change, ISEs should discuss consent again with the person. • It may be appropriate to record the extent to which consent was provided through a consent form or as a note on a client's file. See Chapter 7.2 for guidance on record keeping.

Table 17: Practice guidance on the elements of consent

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

8.2. Reasonable supports

Part 3 of the DVA Act requires ISEs to give at-risk and connected people access to reasonable supports, so that those people can communicate their decision about consent (see Table 7, Chapter 6.4). What is reasonable will depend on various factors.

This legal requirement recognises the best practice approach that organisations need to tailor their processes to accommodate the distinct needs of people who are accessing their services. This is also a key part of trauma-informed service delivery.

The below practice guidance outlines some common approaches to provide access to reasonable supports. However, these supports will depend on the needs of different people, and should be adapted to be responsive to those needs (see Chapter 8.4 for guidance in relation to distinct key cohorts). What is reasonable will also depend on the role of the service provider, and their relationship with the person.

Practice Guidance

Examples of reasonable supports when seeking consent include:

- Providing **access to a support person** such as a cultural liaison officer, community member, family member, or carer when requested or required. The ISE must ensure the support person is not a person of concern or in any way colluding with the person of concern.
- Allowing **sufficient time and space** for the person to consider the information and an opportunity for them, or their support people, to ask questions and raise any concerns. This may include discussions over more than one consultation.
- Providing an interpreter, translator or other communication aid, if needed.
- **Tailoring communication** to the person you are seeking consent from. Make sure you speak to them in an **age-appropriate** way and avoid using jargon or overly complex language.
- Considering whether the person prefers communication to be **verbally or in writing,** or both.
- Engaging with **specialist services** to ensure expert support and advice is available if needed.
- Helping the at-risk person understand the **purpose of information sharing** to support their safety and risk management.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

8.3. Assessing capacity

If an ISE holds a reasonable belief that someone does not have sufficient decision-making capacity to communicate their decision about consent, the ISE may seek consent from another authorised and appropriate person if there is one (see Table 7, Chapter 6.4). This information will support ISEs to assess capacity for adults and young people, when necessary.

An authorised representative may be someone who is authorised by law to act for or represent another person. This may include, among other things:

- Someone who has an enduring power of attorney for another person,
- A guardian within the meaning of the *Public Trustee and Guardian Act 1985.*

ⓘ Remember

ISEs must not seek consent from an authorised representative, if that person is a person of concern in relation to the at-risk person (see Figure 6). The same requirement applies to a person that has parental responsibility for a child or young person (see Figure 7).

Children are presumed to not have capacity, however, under the DVA Act ISEs are required to take into consideration the age, maturity and decision-making ability of the child or young person when dealing with their information (see Chapter 8.4). This reflects the importance of considering the child's views and wishes when dealing with their information, even though children themselves cannot consent to their information being shared under the DFVISS.

Practice Guidance

- In assessing capacity, ISEs may consider whether the person:
  - understands the facts involved
  - understands the main choices
  - is able to weigh up the consequences of the choices
  - understands how the consequences affect them
  - can communicate their decision, views and needs in some way (verbally, in writing or by other means).
- Capacity should be distinguished from the effect of the decision. Just because someone might, in your opinion, make a 'bad' decision does not mean they lack capacity to make that decision.
- Generally, a person will have decision-making capacity if it is possible for the person to make a decision with practicable and appropriate support. See Chapter 8.2 for guidance on reasonable supports.
- ISEs should be aware that a person's decision-making capacity may be impacted by their experiences of DFV, including coercive control.
- Capacity is decision and time specific. This means that the capacity needed for different types of decisions can look different, and capacity can change over time. Someone may have capacity to make some decisions, but not others.
- Capacity assessments should not delay the timely sharing of information.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

8.4. Working with priority cohorts

The DVA Act requires ISEs take into consideration the personal factors of certain cohorts (see Chapter 2.1). This includes:

- the at-risk person's **cultural identity**, **sexual orientation** and **gender identity**, and **religious or spiritual beliefs** (if known).
- if the at-risk person identifies as **Aboriginal or Torres Strait Islander**, the ISE must promote the person's right to self-determination and other cultural rights, and consider the person's family and community connections.
- if the at-risk person is a **child or young person**, ISEs must take into account the age, maturity and decision making ability of the child or young person.

ISEs should always tailor the information sharing process to the needs of each at-risk person. Inequalities, such as gender inequality, colonisation, racism, sexism, ageism, ableism, homophobia and transphobia, can affect an at-risk person's access to appropriate resources and can cause additional reluctance to disclose the violence or engage in a system response. The DFVISS acknowledges that if ISEs don't engage with priority cohorts in a nuanced way, they can inadvertently increase risk to those people, including by generating additional harms through uninformed system responses.

Protocol Requirement

- ISEs must refer to the ACT RAMF for guidance and practice considerations when working with priority cohorts. This includes different practice guidance on intersectionality and system responses, risk screening, assessment and management considerations to promote safer service responses.

Aboriginal and Torres Strait Islander People

Under the DFVISS, ISEs must take into account an Aboriginal or Torres Strait Islander victim-survivors right to self-determination and create opportunities to support self-determination in system responses.

Self-determination is the fundamental right of a people to freely determine their political status and freely pursue their economic, social and cultural development, about matters that impact them.

Practice Guidance

- ISEs should take active steps to support their own understanding of barriers to accessing services and ensure that their policies and procedures support cultural safety.
- Secondary consultation with or direct involvement (with the at-risk person's permission) of an Aboriginal or bi-cultural worker may help ISEs to understand and respond sensitively to the depth of system concerns held by Aboriginal people at-risk of DFV.

LGBTIQA+ communities

LGBTIQA+ people experience distinct types of DFV perpetration, which can be based on their specific identity and driven by systemic discrimination and marginalisation such as homophobia, heterosexism, cissexism and transphobia.

Practice Guidance

- ISEs should consider how their service provision is distinct for communities relating to sexual orientation and gender identity. These different communities have distinct, non-interchangeable needs, health disparities and experiences of DFV.
- ISEs should be aware that a person of concern may use a variety of coercive behaviours to perpetrate harm to LGBTIQA+ communities. For example, a person of concern may threaten to 'out' the at-risk person to family members and/or their workplace or deliberately misgender the at-risk person to control them and enact harm. Please refer to the ACT RAMF.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Children and young people

Children and young people are victim-survivors of DFV in their own right. The DVA Act requires ISEs to consider a child or young person's age, maturity and decision-making ability when sharing information about them.

Practice Guidance

- Interactions with children and young people should be age and developmentally appropriate, while supporting their agency and distinct experience of violence.
- ISEs are encouraged to support the child to contribute to decisions that affect them. This includes engaging with at-risk children when safe, reasonable and appropriate to do so, and seeking their views before sharing their information. Entities who work with children are required to promote the principles of the ACT Child Safe Standards.

Culturally and linguistically diverse communities

People from migrant, refugee or culturally and linguistically diverse backgrounds may face increased risk of exposure to DFV alongside significant barriers to reporting and accessing services. Language barriers, social isolation, community norms, and limited access to trusted networks can be compounded by controlling partners restricting access to information about rights and services.

The DVA Act requires ISEs to take into account a person's cultural identity when sharing information about them.

Practice Guidance

- People from culturally and linguistically backgrounds have distinct and varied needs. Services should seek to understand an individual's distinct cultural identity and experience to shape their service provision.
- Reasonable supports for culturally and linguistically diverse communities may include explaining privacy expectations, learning about and observing different cultural protocols while providing a service response, accommodating no contact requests on days of religious or cultural significance, and providing interpreting and translation services, including phone interpreters.

People with disability

People with disability are more likely to be victim-survivors of DFV than people without disability. They may experience unique forms of abuse, such as threats to withdraw care or restrict mobility, and encounter additional barriers to seeking help.

At-risk people with a disability may experience additional barriers to reporting victimisation, including where they are dependent on the care of others. In some circumstances, the person of concern may be a primary carer of the at-risk person.

Practice Guidance

- Where at-risk people with a disability rely on the care of a person of concern, ISEs need carefully apply the requirements of the DFVISS.
- ISEs should seek to understand the specific needs of the person that may arise from their disability, so that reasonable support can be put in place to support their ability to engage with the service.
- Reasonable supports will depend on the person's needs, and may include taking a multidisciplinary approach with other services and providers, providing plain language explanations, and providing additional time and space to process information and communicate their thoughts.

Older people

Older people may be at higher risk of experiencing distinct types of DFV, including from their adult children as caregivers (known as elder abuse).

When an older person is experiencing elder abuse in DFV setting, risk management considerations can be especially complex. Older people may feel protective of their children, depend on their care, be unable to independently access services, or be unaware of different mechanisms for violence and control (such as technology facilitated financial abuse).

Practice Guidance

- ISEs should be aware of the risk that the older person's carer or family member may be a person of concern. Where possible, ISEs should communicate directly with the older person and support their agency and decision-making in matters affecting them.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

9. INTERACTION WITH OTHER LAWS

This Chapter provides general guidance on how Part 3 of the DVA Act generally interacts with particular Territory and Commonwealth laws. This Chapter also describes provisions in other laws that would no longer restrict information sharing when assessing or managing risk of domestic and family violence.

ⓘ Remember

This Ministerial Protocol should not be relied on as a summary of ISEs' existing obligations under other laws, and it should not be taken as a substitute for legal advice.

Key points

- Sharing information about domestic and family violence is already permitted in certain situations under other laws, including under the *Information Privacy Act 2014* and section 136 of the *Crimes (Sentencing) Act 2005*.
- However, restrictions under these and other laws have contributed to a lack of information sharing culture due to agency concerns about privacy.
- Part 3 of the DVA Act creates a new authorising legal framework to share information, including personal and health information, for a protection purpose. This will now authorise information sharing that may not have always been clearly authorised because of restrictions and cultural barriers to information sharing under other laws (e.g. the *Information Privacy Act 2014* or *Health Records (Privacy Access) Act 1997*).
- Some laws may still restrict how information can be shared under the DFVISS (e.g. *Children and Young People Act 2008)*. This is not common, and most secrecy and confidentiality provisions under other laws will not restrict information sharing under the DFVISS (see Chapter 9.1).
- Where an ISE *receives* information under the DFVISS, that ISE needs to deal with that information using Part 3 of the DVA Act, unless the ISE is authorised to share or use the information for a secondary purpose. Secondary purposes include sharing information under certain other laws (see Chapter 9.2).
- Whenever information received under the DFVISS is shared using another law (a secondary purpose mentioned in Chapter 2.5), the ISE has requirements to notify the Information Sharing Coordinator (see Chapter 4.3). The ISE also has obligations to tell the ISE who they received the information from (see Chapter 2.5), and if the information is about an at-risk or connected person, they must also be notified unless they consented to the disclosure or another exception applies (see Chapter 6.6).
- ISEs may be subpoenaed to produce information they hold, because of information sharing under the DFVISS (see Chapter 9.3).
- To help understand information sharing in the ACT and the general approach to sharing information under various laws, ISEs should refer to Figure 11.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

9.1. DFVISS interaction with other laws

Part 3 of the DVA Act creates a new authorising legal framework to share information, including personal and health information, for a protection purpose. This will now permit information sharing that may not have been previously allowed because of restrictions under other laws (e.g. *Information Privacy Act 2014* or *Health Records (Privacy Access) Act 1997*.

Part 3 of the DVA Act specifically responds to identified legislative barriers for information sharing, that resulted in gaps in information sharing practices.

The DFVISS now gives ISEs the authority to:

- Share information to assess and manage DFV risk, even where the risk level is not yet known or the risk is not imminent.
- Collect and use personal or health information about a person using violence, from sources other than the person themselves, without obtaining their consent.

Most secrecy provisions under various ACT laws do not completely restrict sharing of protected information. A common exception to these secrecy provisions is where sharing the protected information is authorised under another law – which would include the new DFV Information Sharing Scheme legislation. ISEs that work under other legal frameworks should know and apply the secrecy provisions that apply to them. Where other secrecy provisions have exceptions that allow disclosure of protected information under another law, that includes sharing information under the new authorising framework made by Part 3 of the DVA Act.

Case Study 20: when you can share information under the DFVISS

ISE 1 requests risk information from ISE 2. ISE 2 is a Canberra Health Service (CHS) organisation. The *Health Records (Privacy and Access) Act 1997* regulates the sharing of information about people's personal health information. However, the *Health Records (Privacy and Access) Act 1997* permits a person's health information being used for another purpose, if it is required or authorised by another law.

Practically, this means that the information regulated by health records legislation *can be disclosed* under the DFVISS, if the other information sharing requirements under the DFVISS have been met. This means that ISE 2 would not be in breach of its obligations under the *Health Records (Privacy and Access) Act 1997*.

Where other laws have **strict** secrecy or confidentiality provisions, which clearly limit information sharing beyond their own legislative frameworks, that information cannot be shared using Part 3 of the DVA Act. These types of strict secrecy or confidentiality provisions are not commonly found across Territory legislation. In practice, agencies that are ISEs under the DFVISS will have a strong knowledge of the laws that regulate their functions.

Case Study 21: when you cannot share information under the DFVISS

ISE 1 requests risk information from ISE 2. ISE 2 holds information that is considered *sensitive information* under the *Children and Young People Act 2008*. That legislation does not allow sensitive information to be shared under another law.

Practically, this means that ISE 2 is not allowed to disclose certain information to ISE 1, because the information is protected under the *Children and Young People Act 2008*. If ISE 2 shared that information, it would be breaching the provisions of the *Children and Young People Act 2008*.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

9.2. Sharing information under other laws

Nothing in the DFVISS intends to prevent an ISE from collecting, using or disclosing information where it is allowed under another law. Many agencies will continue sharing information under other laws. While this is not an exhaustive list, some of these laws include:

- *Children and Young People Act 2008*
- *Crimes (Sentence Administration) Act 2005*
- *Bail Act 1992*
- *Freedom of Information Act 2016*
- *Information Privacy Act 2014*

However, ISEs need to be aware that once they have received or shared information using Part 3 of the DVA Act, that information generally becomes regulated by the DFVISS. This means that information can then only be shared under other laws if it is for a permitted secondary purpose under the DVA Act (see Table 4, Chapter 2.5). Sharing information for a permitted secondary purpose ensures that information sharing is not unreasonably limited by the DFVISS, and that critical information sharing obligations and powers under other laws are specifically preserved by Part 3 of the DVA Act. This includes mandatory reporting and reportable conduct obligations, which have not been changed by the DFVISS.

ISEs should note that additional laws may be prescribed by a regulation under Part 3 of the DVA Act. For up-to-date information on additional laws prescribed under section 16AI, please refer to the ACT Legislation Register.

Practice Guidance

- If information can lawfully be shared without relying on Part 3 of the DVA Act, organisations and agencies may use existing information sharing laws and mechanisms to do so.
- However, once an ISE *receives or shares* information through the DFVISS, that ISE needs to deal with that information using Part 3 of the DVA Act – unless a permitted secondary purpose applies (see Table 4, Chapter 2.5).
- The permitted secondary purposes preserve critical information sharing obligations and powers under other laws. This includes mandatory reporting and reportable conduct obligations, which have not been changed by the DFVISS.
- To help understand information sharing in the ACT and the general approach to sharing information under various laws, ISEs should refer to Figure 11.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

Can I share information: Information sharing laws in the ACT

Figure 11 describes how privacy laws in the ACT do not stop necessary information sharing. This Figure provides visual guidance on how different types of common scenarios interact with different laws for information sharing.

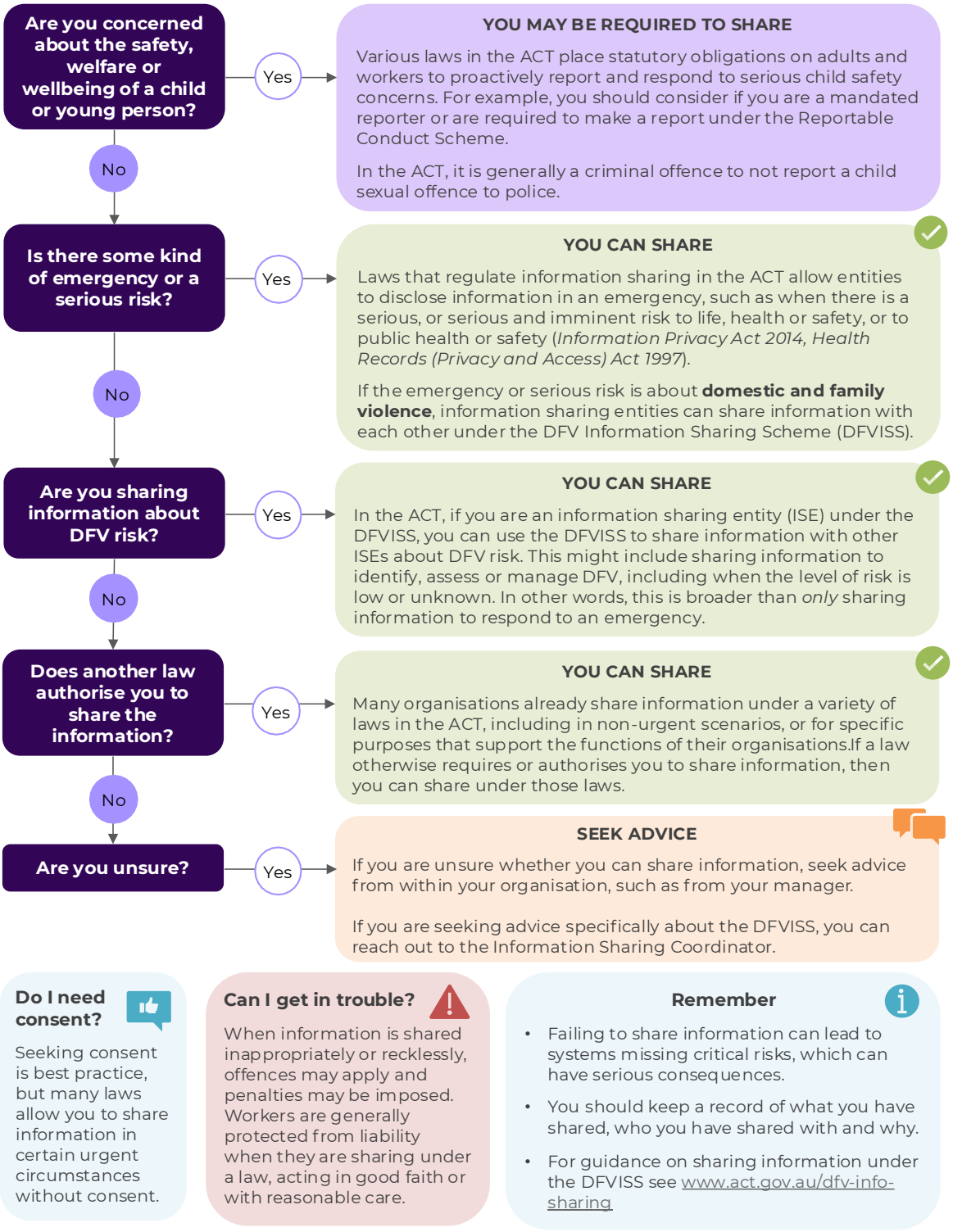


Figure 11: Flowchart - Can I share information? (Information sharing laws in the ACT)

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

9.3. Subpoenas

ISEs may be subpoenaed to produce information they hold because of information sharing under the DFVISS. A subpoena request may relate to case notes, files or any other records. Any party in a court case can ask for a subpoena, whether or not the case relates to domestic and family violence. **ISEs must generally comply with a validly issued subpoena unless the court decides differently**.

Subpoenaed documents do not automatically become evidence in legal proceedings. A court must decide if those documents can be used as evidence. Courts must also consider any objections or challenges to a subpoena. Even if the documents are not used in evidence, the information contained in them and the process of having records subpoenaed can cause harm and distress to a victim-survivor.

Subpoenas can be challenged on a number of grounds, including that it is not relevant, oppressive, vexatious, a 'fishing expedition', it does not demonstrate a legitimate forensic purpose or on the basis of a privilege at law or public interest immunity. A subpoenaed organisation or party **may also object to a subpoena** and ask the court to restrict access to certain documents. Other laws may also apply to the limit the possible scope or validity of a subpoena, for example section 126B of the *Evidence Act 2011* related to protected confidences, and the protection of counselling communications under Division 4.4.3 of the *Evidence (Miscellaneous Provisions) Act 1991*.

Practice Guidance

ISEs are encouraged to:

- carefully read instructions provided on complying with subpoenas, including in relation to producing the documents.
- consider and take steps to manage any potential impact on the safety and wellbeing of victim-survivors as their foremost consideration when deciding whether to challenge or object to a subpoena request.
- seek legal advice on how to respond before producing any information, including to understand whether the subpoena could be validly contested or narrowed.
- notify a victim-survivor that a subpoena has been received where a victim-survivor's record has been subpoenaed.
- refer to the practice guidance in Chapter 7.3. Safe and secure storage of information will support ISEs to identify what records they keep may be relevant to a subpoena request. Special record keeping obligations in Chapter 7.7 will also assist ISEs to identify what information may be captured by a subpoena request.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

10. OFFENCES, LIABILITY AND COMPLAINTS

This Chapter outlines offence and liability provisions under the *Domestic Violence Agencies Act 1986*, including protections for workers and guidance on complaints mechanisms.

Key points

- Similar to other laws regulating the disclosure and use of information, offences and liability may apply to ISEs for unauthorised disclosure or use of information under the DVA Act.
- However, workers who act honestly and without recklessness when dealing with information under Part 3 of the DVA Act have offence and civil liability protections.
- Good record keeping practices (in accordance with Chapter 7) will support ISEs to show how they have complied with the requirements of the DFVISS.
- ISEs are encouraged to align their existing complaints policies and procedures to receive complaints in relation to privacy breaches and decisions made under the DFVISS. This includes ISEs who are covered by relevant Territory or Commonwealth laws.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au

10.1. Offence for reckless disclosure or use

If information is shared inappropriately, offences may apply and penalties may be imposed. There are two offences under Part 3, relating to the **reckless disclosure** or **use of shared information**. Shared information refers to information about a person that is disclosed to, or obtained by, an information holder because of the operation of the DFVISS.

A person dealing with information under the DFVISS will not be committing an offence if:

- The disclosure or use occurs as authorised under Part 3 of the DVA Act; or
- The disclosure or use is required as part of a court proceeding; or
- The disclosure or use occurs with the person's consent; or
- The disclosure is to the Police in connection with a possible family violence offence.

10.2. Protection for workers

A person who is authorised to share information under the DFVISS, who acts in good faith and with reasonable care will not be held:

- Liable for any criminal, civil or disciplinary action for providing information as allowed under Part 3 of the DVA Act
- To have breached any code of professional ethics or any accepted standards of professional conduct.

Generally, a practitioner may be considered to have acted honestly and without recklessness when they

- Share information in accordance with their obligations, functions and authorisations
- Intend for the information to be shared for a protection purpose under Part 3 of the DVA Act
- Do not act maliciously, recklessly or negligently when exercising their power to share information.

Individual workers will generally be held to a standard based on their own knowledge, skills and experience. Record keeping will help individual workers and entities show how they have complied with the requirements of the DFVISS (see Chapter 7).

10.3. Complaints

ISEs should align their existing complaints policies and procedures to receive complaints in relation to activities and decisions made under the DFVISS. Complaints procedures should be made available so that people are aware of their right to make a complaint.

Complaints about how an organisation is applying the Scheme would be made, in the first instance, directly to the ISE involved. Records of complaints should be kept. See Chapter 7 for further information.

Privacy complaints may also be made under Territory and Australian privacy laws, if an ISE is covered by those laws. If this applies to an ISE, that ISE must make those complaint pathways known.

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au



ACT Government

Authorised by the ACT Parliamentary Counsel—also accessible at www.legislation.act.gov.au