# Family violence information sharing scheme, information sharing by Support and Safety Hubs and privacy law in Victoria

## Frequently Asked Questions

## Introduction

The family violence information sharing scheme came into effect in February 2018. The scheme made a number of amendments to the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Health Records Act 2001* (**HR Act**).

The scheme forms part of the legislative response to the recommendations of the Royal Commission into Family Violence. This scheme is designed to minimise the legislative barriers that had previously prevented the timely and effective sharing of information in cases of family violence.

This Frequently Asked Questions (**FAQs**) document has been prepared for practitioners who have a role in assessing and managing family violence risk.[1] The intention of these FAQs is to provide an overview of the relevant changes to the PDP Act and the HR Act and consider how they operate within the wider family violence information sharing scheme.

For further information on any of the topics covered in this document please refer to the Ministerial *Family Violence Information Sharing Guidelines* (**the Guidelines**) published by Family Safety Victoria. The Guidelines are issued by the responsible Minister and are legally binding, applying to all information sharing entities (**ISEs**).

### 1. Privacy law in Victoria: What are the existing obligations for Victorian public sector organisations?

The new family violence information sharing scheme is designed to operate within the existing privacy obligations under the PDP Act and HR Act.

Victorian public sector organisations, including contracted service providers of the Victorian government and local councils, have ongoing obligations to protect the personal information of individuals under the PDP Act.[2] Where a Victorian public sector organisation collects, holds, uses or discloses personal information, it must adhere to the 10 Information Privacy Principles (**IPPs**), listed in Schedule 1 of the PDP Act. The IPPs set out the minimum standards for how the Victorian public sector should handle personal information, including the types of information they are required or permitted to collect, how that information is used and shared, how the information is protected, and for how long the information will be retained.

Victorian public sector organisations and private organisations holding health information have obligations to protect the health information of individuals under the HR Act.[3] The HR Act contains 11 Health Privacy Principles (**HPPs**) that set the minimum requirements for the handling of health information throughout its lifecycle, similarly to the IPPs under the PDP Act.

Victorian public sector organisations may also have obligations to ensure the security of any public sector data (including personal information) that they may hold. This involves adherence to the Victorian Protective Data Security Framework (**VPDSF**) and Victorian Protective Data Security Standards (**VPDSS**).[4]

**Appendix B** of these FAQs lists a number of resources to assist practitioners to understand their overarching privacy obligations under Victorian privacy law.

## Changes to the privacy landscape under the scheme

### 2. How does the scheme operate?

Part 5A of the *Family Violence Protection Act 2008* (**FVP Act**) relates specifically to information

[1] The term 'practitioner' is used throughout this FAQs document to refer to workers who have a role in assessing and managing family violence risk under the scheme.
[2] Personal information is defined in s 3 of the PDP Act.
[3] Health information is defined in s 3 of the HR Act.
[4] See Part 4 of the PDP Act for the organisations that are required to comply with the VPDSF and VPDSS. Further detail on the VPDSF and VPDSS can be found on OVIC's website.

sharing and includes provisions that require and permit the collection, use or disclosure of confidential information (including personal information and health information) for family violence assessment or protection (risk management) purposes. These purposes are defined in the FVP Act and are set out in Question 12 below. The information may relate to victim survivors, perpetrators or alleged perpetrators, and third parties[5] (such as previous partners, friends or neighbours of either a victim survivor, perpetrator or alleged perpetrator).

As an initial point of reference, if information could already be shared under existing arrangements or laws, including privacy laws, then entities prescribed under the scheme may continue to share under these laws and the provisions of Part 5A **do not need to be met before sharing the information.** For example, a law enforcement agency with the authority to share personal information under s 15 of the PDP Act can continue to share that information for relevant purposes without needing to rely on Part 5A of the FVP Act.

### 3. Do the Information Privacy Principles and Health Privacy Principles still apply?

Yes. The scheme only provides limited exceptions or modifications from the IPPs and HPPs. Practitioners should always have regard to their existing obligations under their enabling legislation and the PDP Act and HR Act when sharing information under the scheme and beyond a family violence context.

### 4. What are the amendments to the PDP Act and HR Act?

Legislative reforms remove the word 'imminent' from the 'serious and imminent threat' exception where it features in a number of the IPPs and HPPs:

- **IPP 2.1(d)(i)** permits the use or disclosure of personal information for a secondary purpose where an organisation[6] reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare.
- **IPP 6.1(a)** states that an organisation is not required to provide an individual with access to their personal information where providing access would pose a serious threat to the life or health of any individual.
- **IPP 10.1(c)** permits an organisation to collect sensitive information where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, and the individual whom the information is about is physically or legally incapable of consenting to the collection.
- **HPP 1.1(f)(i)** permits the collection of health information in the absence of consent where the collection is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual.
- **HPP 2.2(h)(i)** permits the use or disclosure of health information for a secondary purpose in the absence of consent where an organisation[7] reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare.

The previous requirement that a threat be 'imminent' as well as 'serious' before information could be shared or released set a higher threshold that was difficult for practitioners to interpret and establish. This amendment applies to the above IPPs and HPPs and is not specific to

[5] 'Perpetrator' is defined as 'person of concern' in s 144B of the FVP Act. Third parties are defined as 'linked persons' under s 144A of the FVP Act. 'Victim survivor' is the terminology adopted by the Royal Commission into Family Violence and the Guidelines to describe a 'primary person', which is defined in s 144E of the FVP Act as a person that an information sharing entity reasonably believes as at risk of being subjected to family violence.

[6] As defined in s 3 of the PDP Act.

[7] As defined in s 3 of the HR Act.

the family violence context. The Office of the Victorian Information Commissioner (**OVIC**) and Health Complaints Commissioner (**HCC**) have co-published guidance on the removal of 'imminent' from the IPPs and HPPs, available on their respective websites.

### 5. How does the scheme modify the application of the IPPs and the HPPs?

The scheme provides for a number of exceptions or modifications to the IPPs and the HPPs:

- **Information Sharing Entities** (**ISEs**) and the **Central Information Point** (**CIP**)[8] are exempt from complying with **IPPs 1.4 and 1.5**[9] when collecting information about perpetrators (including alleged perpetrators), and concurrently from **HPPs 1.3 and 1.5**.[10] The purpose of these exceptions is to ensure that ISEs are not required to collect personal information directly from a perpetrator or alleged perpetrator, nor provide notice of collection where information about a perpetrator or alleged perpetrator has been collected from a third party. These changes recognise that it may not always be safe, reasonable or appropriate for practitioners to collect information directly from a perpetrator or alleged perpetrator, and that there may be safety risks involved with notifying these individuals that their information has been collected from another source.
- The CIP is expressly exempt from **IPP 6 and HPP 6**,[11] meaning that the CIP is not required to provide access to or correct personal information and health information about an individual that the CIP has collected for the purposes of the new Part 5A of the FVP Act. The CIP is designed to act as a conduit for information held by other ISEs, who are better placed to determine whether a request for access or correction could pose a risk of harm to victim survivors.
- An ISE may refuse access to information under **IPP 6 or HPP 6** where a family violence risk has been established, if the individual making the request is a perpetrator or alleged perpetrator.[12] This change provides ISEs with a greater ability to ensure that victim survivors are not unduly exposed to increased risk by way of perpetrators accessing information about them.[13]

In addition to the above exceptions from the IPPs under the scheme, the *Victorian Data Sharing Act 2017* makes an amendment to **IPP 10.1(b)**, which allows entities to collect sensitive information where either authorised or required by law. In the context of family violence information sharing, this means that ISEs are not required to obtain consent from a perpetrator or alleged perpetrator before collecting sensitive information about them (such as criminal record information). ISEs are also not required to gain consent from any person before collecting sensitive information about them in relation to a child victim survivor.

---

[8] The CIP is a secure, state-wide service that will collate information relevant for family violence risk assessment and risk management purposes, operated by Family Safety Victoria. For more information on the CIP, please visit Family Safety Victoria's website.

[9] Under the new s 15A of the PDP Act.

[10] Under the new s 14B of the HR Act.

[11] Under the new s 15A of the PDP Act and the new s 14B of the HR Act, respectively.

[12] Under the new s 144QA of the FVP Act.

[13] Where it is safe to do so, an ISE may grant a request for access or correction under IPP 6 from a perpetrator (for example, where a person has been incorrectly identified as a perpetrator of family violence and wishes to correct any records accordingly). Where a perpetrator has been incorrectly identified and does not present a risk of committing family violence, their rights of access and correction will be the same as for any other person under the scheme. See page 114 of the Guidelines for more information.

## 6. How does the scheme amend the *Freedom of Information Act 1982* (Vic)?

***Access to personal affairs information***

Section 33 of the *Freedom of Information Act 1982* (Vic) (**FOI Act**) deals with access to documents containing personal affairs information where disclosure of the information would not involve unreasonable disclosure.

Section 33(2) provides that an exception to the 'unreasonable disclosure' test when the request for access is made by a person who seeks access to a document containing their personal affairs information. Generally speaking, this means that an individual will be granted access to a document containing their personal affairs information, subject to an exception relating to health information.[14]

A new sub-section 33(2AB) has been inserted into s 33(2) of the FOI Act, requiring that:

- when an ISE or a Minister receives a request from a person who is a perpetrator or an alleged perpetrator of family violence (the applicant); and
- the applicant is seeking access to documents containing their personal information; and
- when the agency or Minister is determining whether disclosure of the applicant's personal affairs would involve the unreasonable disclosure of information relating to the personal affairs of any person, the agency or Minister must also take into account whether the disclosure would increase the risk to a primary person's safety from family violence.[15]

***Neither confirming or denying the existence of a document***

Section 27(2) of the FOI Act provides that an agency or a Minister is not required to disclose the existence of an exempt document in certain circumstances. For example, a law enforcement document that relates to a current covert investigation.

A new subsection 27(2)(ab) has been inserted into s 27(2) of the FOI Act which provides that an agency or a Minister is not required to confirm or deny the existence of any document, if confirming or denying the existence of that document would involve the unreasonable disclosure of information relating to the personal affairs of any person for the reason that it would increase the risk to the safety of a victim survivor[16] of family violence.

Documents in the possession of the CIP are exempt from FOI, to the extent that they would disclose personal information or health information about a victim survivor, a perpetrator or a relevant third party.[17]

For further information regarding requests to access information under the FOI Act, practitioners should refer to Chapter 10 of the Guidelines.

## 7. What about ISEs that are bound by the Commonwealth *Privacy Act 1988*?

If an ISE has obligations under the Commonwealth *Privacy Act 1988,* they must continue to comply with the Australian Privacy Principles (**APPs**) when sharing information under Part 5A. Practitioners should refer to Chapter 11 of the Guidelines for more detail on sharing information in accordance with the APPs under the scheme.

[14] See s 33(4) of the FOI Act.
[15] Under the new s 33(2AB) of the FOI Act.
[16] A victim survivor can include: an affected family member, a child, or a protected person.
[17] Under the new s 144QE of the FVP Act.

### 8. Can organisations not bound by the PDP Act or *Privacy Act 1988* have privacy obligations?

Yes. ISEs not already bound by the information privacy provisions of the PDP Act or the Commonwealth *Privacy Act 1988* are required to handle personal information and unique identifiers in accordance with Part 3 of the PDP Act, including adherence to the IPPs. ISEs subject to the Commonwealth *Privacy Act 1988* will continue to be bound only by that Act.[18]

This ensures that appropriate privacy protections are in place under the scheme and that all ISEs are subject to the complaints provisions of either the PDP Act or the Commonwealth *Privacy Act 1988* (where applicable) in relation to alleged interferences with privacy. Privacy complaints are discussed further in Question 19. Victorian entities holding health information continue to be bound by the HR Act.

As part of these privacy obligations, information sharing entities need to comply with IPP 4, requiring them to take reasonable steps to protect the information (including personal information) they access or hold. Reasonable steps include undertaking the following activities across the information lifecycle:

- identifying and understanding information types;
- assessing and determining the value of the information;
- identifying the security risks to the information;
- applying security measures to protect the information; and
- managing the information risks.

For more information on these requirements, please refer to the data security resources available on OVIC's website.

**Appendix B** of these FAQs lists a number of resources to assist practitioners to understand the overarching privacy obligations under the PDP Act.

## Information sharing by Support and Safety Hubs

### 9. What are the amendments to the privacy landscape relevant to Support and Safety Hubs?

***Notice of collection***

Support and Safety Hubs, known as 'The Orange Door,' help women, children and young people experiencing family violence and families who need support with the wellbeing and development of their children. The Support and Safety Hubs also deliver perpetrator services, aimed at challenging and changing perpetrators' behaviour.

Support and Safety Hubs are not required to comply with IPPs 1.3, 1.4 and 1.5 and concurrently HPPs 1.3, 1.4 and 1.5 when collecting personal or health information (respectively) for the purposes of Part 5B of the FVP Act (relating to information sharing by Support and Safety Hubs).[19] In practice, this means that Support and Safety Hubs will not be required to provide notice of collection to an individual when collecting their personal or health information, either directly from them or from a third party.

***Access to information***

Support and Safety Hubs may refuse access to confidential information under **IPP 6** or **HPP 6**

[18] See, s 144QB of the FVP Act and Chapter 11 of the Guidelines

[19] Under the new ss 15A(1A) of the PDP Act and 14B(2A) of the HR Act, respectively. More information about Support and Safety Hubs can be found on Family Safety Victoria's website.

where the Support and Safety Hub believes on reasonable grounds that granting an individual access to the information would increase a risk to the safety of a child or group of children, or if the information is confidential information about a perpetrator or alleged perpetrator and giving the individual access to the information would increase the risk to a victim survivor's safety from family violence.[20]

## Information sharing in practice

### 10. Can information already be shared under Victorian privacy law?

Despite common perceptions that privacy law acts as a barrier to information sharing, the PDP Act and HR Act have always facilitated information sharing in certain circumstances. Such cases may include where there is a serious threat to the life, health, safety or welfare of an individual or the public; where the disclosure is authorised or required by law; or where the individual has consented. As a starting point, IPP 2 and HPP 2 set out a number of instances where an organisation may share an individual's personal information or health information for a secondary purpose (a purpose other than the primary purpose for collection).

If an ISE was able to lawfully share information under the PDP Act or HR Act prior to being prescribed as an ISE, **they may continue to do so under those laws.** For guidance on how to share personal information within existing privacy obligations, practitioners should refer to the *Guidelines for sharing personal information*, available on OVIC's website. Guidance on complying with the HR Act requirements is available on the HCC's website.

### 11. What if an entity is not a prescribed ISE but wishes to share information about family violence risk?

In some cases, a Victorian public sector organisation that is **not** a prescribed ISE under the scheme may wish to share family violence information that they hold with another entity, whether that entity is a prescribed ISE or not. Similarly, an ISE may wish to share family violence information with an entity that is **not** a prescribed ISE under the scheme. If an organisation is not a prescribed ISE, this does not necessarily mean that they cannot share or receive family violence information.

In these cases, practitioners can rely on provisions that require or permit information sharing in their own enabling legislation, or the authorisations under IPP 2.1 and HPP 2.2 to share the relevant information. Recipients of the information should also ensure that they have the legal authority to collect it, either under their own enabling legislation, the PDP Act or the HR Act.

### 12. Who can share information under the scheme?

There are a number of entities prescribed as ISEs under the *Family Violence Protection (Information Sharing and Risk Management) Regulations 2018* (**Regulations**). Practitioners should refer to the list of prescribed ISEs contained in Part 2 of the Regulations to determine which entities will be able to share information under the scheme.[21]

ISEs that are prescribed under the Regulations as **risk assessment entities (RAEs)** can request and disclose information for a **family violence risk assessment purpose**, that is, to establish and

[20] Under ss 144SG(1) and (2) of the FVP Act.
[21] See also the list of ISEs on page 38 of the Guidelines.

assess a risk of family violence. All ISEs are permitted to share information with RAEs for a family violence assessment purpose.[22]

RAEs are a subset of ISEs, prescribed based on their functions. Examples of ISEs that are prescribed as RAEs include specialist family violence services, Victoria Police, and services forming part of The Orange Door (the Support and Safety Hubs).

All ISEs under the scheme will be able to share information for a **family violence protection purpose**, that is, to manage a risk of family violence. Examples of key entities that can share information for a protection purpose include Magistrates' Court officials, Children's Court officials, Corrections Victoria and the Adult Parole Board.

It is important to note that courts and tribunals prescribed as ISEs will be exempt from Part 5A in relation to their **judicial or quasi-judicial functions**, to mirror the existing exemption for courts and tribunals under s 10 of the PDP Act and s 14 of the HR Act.

### 13. What types of information can be shared?

ISEs can share **'confidential information'** under Part 5A. Confidential information is an umbrella term that includes:

- health information and identifiers for the purposes of the HR Act
- personal information for the purposes of the PDP Act, including sensitive information (such as a criminal record), and unique identifiers.

However, s 144C of the FVP Act sets out types of information deemed to be **'excluded information'** under the scheme, which **cannot** be shared. Examples of when information will be deemed excluded information include if the collection, use or disclosure of the information could be reasonably expected to:

- endanger a person's life or result in physical injury
- contravene a court order or legal professional privilege, or
- be contrary to the public interest, amongst others.[23]

In determining whether information is excluded information under the scheme, practitioners should refer to the list of excluded information in Chapter 1 of the Guidelines, or seek independent legal advice where necessary.

### 14. How can practitioners determine quickly when to share information?

Some tips to assist practitioners to determine if and when they can share information include:

- verify the identity of the ISE before sharing – this can be done by confirming that the requesting ISE has been prescribed under the Regulations[24]
- consider whether the information is relevant to assessing or managing a family violence risk[25]
- consider whether the information is excluded information[26]
- ensure that the relevant consent thresholds have been met[27]
- refer to any obligations under enabling legislation and privacy laws to ensure that any sharing of information under the scheme is done in accordance with the relevant privacy requirements

[22] See page 25 of the Guidelines.
[23] See s 144C of the FVP Act and page 32 of the Guidelines for a full list of the types of information deemed 'excluded information'.
[24] See page 38 of the Guidelines.
[25] See Chapter 1 of the Guidelines.
[26] As above.
[27] See Question 17 below for an outline of the conditions for consent under the scheme. Practitioners should also refer to Chapter 9 of the Guidelines for more information regarding consent provisions.

- check that the information does not contravene other laws[28]
- seek to align existing internal information management policies and practices with the scheme to facilitate quick decision making.[29]

For further guidance practitioners should refer to the Guidelines and resources available on Family Safety Victoria's website.

### 15. How can practitioners share information under the scheme?

***Family violence risk assessment purpose***

A RAE can request information about a victim survivor, a perpetrator or alleged perpetrator, and a third party from an ISE for a **family violence assessment purpose**. The primary focus when sharing information for a family violence assessment purpose is establishing whether a risk of family violence is present, assessing the level of risk the alleged perpetrator or perpetrator poses to the victim survivor, and correctly identifying the parties as perpetrator or victim survivor.[30]

ISEs must disclose confidential information to a RAE that has requested the information about an individual for a family violence assessment purpose.[31] This means that ISEs will be required to share information, provided that:

- the information is not excluded information
- the disclosure does not contravene another law
- the relevant consent provisions have been adhered to[32]
- the ISE is not acting in their judicial or quasi-judicial function.

***Family violence protection purpose***

An ISE may request and share confidential information with another ISE for a **family violence protection purpose**. Under the scheme, 'family violence protection purpose' means managing the risk of the perpetrator committing family violence, or the risk of the victim survivor being subjected to family violence.[33] An ISE that receives a request must share relevant information provided the ISE **reasonably believes** that the disclosure is necessary for a protection purpose and:

- the information is not excluded information
- the disclosure does not contravene another law
- the relevant consent provisions have been adhered to
- the ISE is not acting in in their judicial or quasi-judicial function.

Sharing information about alleged perpetrators is not permitted for a protection purpose.[34] This is because the family violence risk should already be established and the identity of the perpetrator known. When sharing information about a perpetrator for a protection purpose, an ISE will need to have established who the perpetrator is and clearly distinguish them from the victim survivor. In determining the identity of a perpetrator, ISEs should refer to Chapter 3 of the Guidelines.

[28] See Chapter 11 of the Guidelines.
[29] See Chapter 1 of the Guidelines for an overview of Part 5A. Other matters practitioners should have regard to include; available staff training and the new Family Violence Risk Assessment and Risk Management Framework.
[30] See Chapter 1 of the Guidelines. Appendix A and B of the Guidelines also provide checklists for practitioners, that provide guidance on considerations that ISEs must take into account when making or responding to a request for information under the scheme.
[31] See Division 2 of Part 5A of the FVP Act.
[32] Under Division 5 of Part 5A of the FVP Act.
[33] See page 21 of the Guidelines.
[34] See page 28 of the Guidelines.

**16. Can ISEs voluntarily share information with other ISEs or victim survivors?**

Yes. The scheme encourages the proactive sharing of information between ISEs. An ISE may voluntarily disclose confidential information to a RAE for a risk assessment purpose[35] and may voluntarily disclose confidential information to another ISE for a protection purpose.[36] Any information shared must not be excluded information and disclosures must be permitted under the consent provisions in Division 5, Part 5A of the FVP Act.

An ISE may also voluntarily disclose confidential information about a perpetrator to a victim survivor (including a child victim survivor or parent of a child victim survivor, so long as the parent of the child is not a perpetrator), to allow the victim survivor to manage the risk of the person of concern committing family violence.[37] However, a victim survivor may only use this information to manage the risk of family violence.

Additionally, ISEs may proactively disclose confidential information to the CIP in a number of circumstances. For further information on the CIP, see Family Safety Victoria's website.

## Important considerations when sharing information

**17. Do practitioners need to seek the consent of an individual before sharing information about them?**

Not in every case. Practitioners should refer to Chapter 9 of the Guidelines to help determine whether there is a need to seek consent before sharing information. As an overview:

- Consent is not required for ISEs to share information about a perpetrator or alleged perpetrator.[38]
- When sharing information about a **victim survivor who is an adult**, an ISE should seek the consent of the adult before sharing information.[39] However, consent is *not* required if the ISE reasonably believes that the collection, use or disclosure of the confidential information is necessary to lessen or prevent a serious threat to life, health, safety or welfare.
- An ISE should seek the consent of a **third party** before sharing confidential information about them.[40] However, this can be done without consent where an ISE reasonably believes that the disclosure of information is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare.
- ISEs may share information without the consent of any person where the **victim survivor is a child**, and the information is relevant to assessing or managing the risk of family violence posed to the child victim survivor. In this instance, the sharing of information must be necessary for a family violence risk assessment or protection purpose concerning a child victim survivor. An ISE must comply with the Guidelines when sharing confidential information about a child, and practitioners should have regard for the agency of the child and other family members at risk of family violence before sharing information, by ensuring their views are sought and taken into account.[41]

It is important to note that under the Regulations, ISEs are required to keep a record of disclosures of confidential information under the

[35] See s 144KA of the FVP Act.
[36] See s 144LA of the FVP Act.
[37] See s 144M of the FVP Act.
[38] Under s 144N of the FVP Act.
[39] The five elements of consent for the purposes of the scheme are contained in Chapter 9 of the Guidelines.
[40] See s 144NB of the FVP Act.
[41] Under s 144J(3)(a) of the FVP Act.

scheme, including a record of whether or not consent was gained from a victim survivor who is an adult or a third party, before sharing confidential information about them. ISEs are also required to keep a record of whether the views of a child victim survivor or their parent were taken into account before sharing information under the scheme. Practitioners should refer to Chapter 10 of the Guidelines for further information on recordkeeping.

### 18. How does the scheme deal with unauthorised sharing of confidential information?

In order to protect confidential information, the scheme includes offences for unauthorised, or intentional or reckless sharing of confidential information.[42] Unauthorised sharing of information carries a fine of 60 penalty units for individuals (300 for a body corporate), and intentional or reckless sharing of information carries a fine of 600 penalty units and/or up to 5 years imprisonment for individuals (and 3000 penalty units for a body corporate).

Practitioners will be protected from these offences under the scheme if they acted **in good faith and with reasonable care** in sharing the confidential information. This protection applies only to individuals and not to organisations. A practitioner who acts in good faith and with reasonable care when sharing information will also not be held to have breached any code of professional ethics or to have departed from accepted standards of professional conduct.[43]

A practitioner will not have committed an offence merely for sharing information in a way that is not compliant with the Guidelines. However, non-compliance with the Guidelines may be taken into account where a privacy complaint is made to OVIC or to the HCC.

The enforcement provisions in Division 9 of Part 3 of the PDP Act apply to organisations. Where a privacy complaint raises a serious or flagrant breach of privacy by an ISE, OVIC may issue a compliance notice to that ISE under s 78 of the PDP Act. It is an offence for an organisation not to comply with a compliance notice, carrying a fine of 600 penalty units for an individual or 3000 penalty units for a body corporate.[44]

The HCC may also serve a compliance notice on organisations for serious or flagrant contraventions of the HR Act under s 66 of the HR Act. It is an offence not to comply with a compliance notice, carrying a fine of 3000 penalty units for a body corporate or 600 penalty units in any other case.[45]

### 19. What can an individual do if they believe their information has been shared inappropriately?

If an individual believes that their personal information or health information has been mishandled under the scheme, they can make a complaint. OVIC can deal with complaints concerning a breach of one or more of the IPPs under the PDP Act. Individuals can complain to the HCC where they suspect a breach involving their health information. Complaints should be directed to the relevant ISE in the first instance before a formal, written complaint is lodged with either OVIC or the HCC.

OVIC and the HCC can only deal with complaints about an entity that falls within the scope of the PDP Act or the HR Act respectively. If a person has a privacy complaint regarding the handling of their personal information or health information by an entity covered by the *Privacy Act 1988*, the complaint should be directed to the Office of the Australian Information Commissioner.

Organisations and individuals can refer to the OVIC website or HCC website for guidance on

[42] See Division 9 of Part 5A of the FVP Act.
[43] See Chapter 12 of the Guidelines.
[44] Under s 82 of the PDP Act.
[45] Under s 71 of the HR Act.

how to make a complaint and may contact each office for further assistance.

*This document should be read with Family Safety Victoria's Ministerial Guidelines on the scheme. For more information on the scheme, please refer to the Guidelines.*

## Appendices

### Appendix A: Useful terms and acronyms

*An **alleged perpetrator*** is a person who is alleged to pose a risk of committing family violence.

*The **Central Information Point (CIP)*** is a secure, state-wide service that will collate information relevant to family violence risk assessment and risk management.

***Confidential information*** includes health information and identifiers for the purposes of the HR Act and personal information for the purposes of the PDP Act, including sensitive information, identifiers and unique identifiers, under s 144A of the FVP Act.

***Family violence assessment purpose*** is defined under s 144A of the FVP Act to mean the purpose of establishing or assessing the risk of a person committing family violence or a person being subjected to family violence.

***Family violence protection purpose*** is defined under s 144A of the FVP Act to mean the purpose of managing a risk of a person committing family violence (including the ongoing assessment of the risk of the person committing family violence) or a person being subjected to family violence (including the ongoing assessment of the risk of the person being subjected to family violence).

***Information sharing entity (ISE)*** is defined under s 144D of the FVP Act to be a person or body prescribed, or a class of person or body prescribed, to be an information sharing entity.

***Perpetrator*** is defined as a person of concern under s 144B of the FVP Act if an information sharing entity reasonably believes that there is a risk that the person may commit family violence.

*A **risk assessment entity (RAE)*** is an information sharing entity prescribed to be a risk assessment entity. Risk assessment entities can request and receive voluntary disclosures from ISEs for a family violence assessment purpose.

***Share***, for the purposes of this document and the Guidelines, means the collection use and disclosure of information.

***Support and Safety Hubs,*** known as 'The Orange Door', help women, children and young people experiencing family violence and families who need support with the wellbeing and development of their children. Support and Safety Hubs also provide services aimed at perpetrators, to challenge and change their behaviour.

***Third party (defined as a linked person*** under s 144A of the FVP Act) is any person whose confidential information is relevant to a family violence assessment purpose or family violence protection purpose other than a person who is a victim survivor, or a perpetrator or alleged perpetrator.

***Victim survivor*** is defined in s 144E of the FVP Act as a person that an information sharing entity reasonably believes as at risk of being subjected to family violence. Victim survivors are referred to as primary persons (adult or child) under the Amending Act.

### Appendix B: Other resources

The following is a list of key resources available on OVIC's website. Prescribed ISEs should refer to these resources for more information on their overarching privacy obligations, drafting a privacy

policy or collection notice, undertaking privacy impact assessments and understanding their data security obligations.

- Guidelines for sharing personal information
- Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1
- Guidelines to the Information Privacy Principles
- Information Sheet: Collection Notices
- Information Sheet: Drafting a Privacy Policy
- Privacy By Design Background Paper
- Privacy Impact Assessment introduction and template
- Responding to Privacy Breaches Guidelines
- Responding to Privacy Breaches Checklist
- Victorian Protective Data Security Framework
- Victorian Protective Data Security Standards

## Further Information

**Victorian Information Commissioner**

**t:** 1300 00 6842
**e:** enquiries@ovic.vic.gov.au
**w:** ovic.vic.gov.au

**Health Complaints Commissioner**

**t:** 1300 582 113
**e:** hcc@hcc.vic.gov.au
**w:** hcc.vic.gov.au



Version 1.1, issued January 2019