Office of the Victorian Information Commissioner

Overview

Freedom of Information | Privacy | Data Protection

Overview

On this page

Document version: Overview 2020, 3 December 2020.

Introduction to these Guidelines

O.1 Under the Victorian *Privacy and Data Protection Act 2014* (**PDP Act**), the Information Commissioner has the function of issuing guidelines for the Information Privacy Principles (**IPPs**).[1] The IPPs outline the minimum standard for the collection, storage, handling, use, disclosure and destruction of personal information by Victorian public sector (**VPS**) organisations. The IPPs are relevant for all VPS organisations, as well as some private or community sector organisations where those organisations are carrying out functions under a State contract with a Victorian public sector organisation.[2]

O.2 These Guidelines are intended for individuals working with the IPPs under the PDP Act. They indicate how the Information Commissioner interprets and applies the IPPs, and the matters that the Information Commissioner may consider when advising organisations during consultations, dealing with complaints, or examining acts and practices or breaches during an investigation. They also provide guidance to organisations on the broad application of the IPPs and how to embed privacy protections in workplace culture and practices.

O.3 These Guidelines are not legally binding and do not constitute legal advice about how an organisation must comply with the IPPs in specific circumstances. Ultimately, organisations must decide how to interpret and apply the IPPs in a manner that is consistent with the PDP Act. Organisations should consult their privacy officer or unit, or seek legal advice, as appropriate.

O.4 Organisation may also contact OVIC with queries about the IPPs or the Guidelines. However, OVIC can only provide guidance of a general nature.

O.5 These Guidelines should be read together with the full text of the IPPs. In practice, the IPPs often interact. The application of the IPPs can differ depending on the context of the situation, so organisations should apply the IPPs on a case by case basis.

Objects of the PDP Act and the Information Lifecycle

O.6 Organisations should apply the IPPs with the objects of the PDP Act in mind.[3] They are:

- to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
- to balance the public interest in promoting open access to public sector information with the public interest in protecting its security;
- to promote awareness of responsible personal information handling practices in the public sector;
- to promote the responsible and transparent handling of personal information handling in the public sector; and
- to promote responsible data security practices in the public sector.

O.7 The PDP Act and the IPPs imply some shift in control from the collectors and users of personal

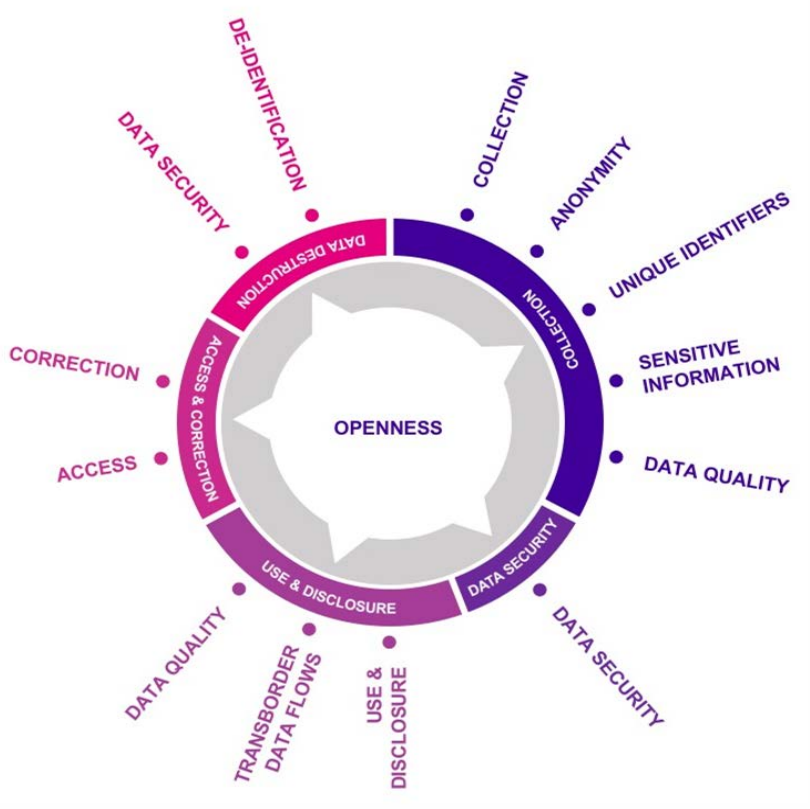
[1] PDP Act, s 8C(1)(g).

[2] See also: *Guidelines for outsourcing in the Victorian public sector Accompanying guide*, OVIC, May 2017.

[3] PDP Act, s 5.

information to the sources and subjects of it. However, it is not a total shift. As the objects of the PDP Act outline, it is a balancing of various public interests.

O.8 The IPPs govern the collection, use, disclosure, and destruction of information throughout the information lifecycle. This is illustrated in the following diagram, which indicates where in that lifecycle each of the ten IPPs is most relevant.



When do the IPPs apply?

Which organisations are covered by the PDP Act?

O.9 Section 13 of the PDP Act provides a list of the categories of bodies and persons who are subject to Part 3 of the PDP Act and must comply with the IPPs. These are:

a. Ministers;
b. Parliamentary Secretaries, including the Parliamentary Secretary of the Cabinet;
c. public sector agencies, meaning public service bodies or public entities within the meaning of the *Public Administration Act 2004* (Vic) (this includes Victorian government departments);
d. local councils;
e. bodies established or appointed for a public purpose by or under an Act (such as Victorian public universities);
f. bodies established or appointed for a public purpose by the Governor in Council, or a Minister, otherwise than under an Act;
g. persons holding an office or position established by or under an Act (other than the office of a member of the Parliament of Victoria) or to which the person was appointed by the Governor in Council, or a Minister, otherwise than under an Act (such as the Victorian

Ombudsman);

h. courts or tribunals;
i. Victoria Police;
j. a contracted service provider, but only in relation to its provision of services under a State contract which contains a provision of a kind referred to in s 17(2) of the PDP Act;[4] and
k. any other body that is declared by an order published in the Government Gazette to be an organisation covered under the PDP Act.

O.10 These categories of bodies and persons are 'public sector organisations' for the purpose of Part 3 of the PDP Act. The starting point for these organisations is that they need to act in accordance with the IPPs.[5] However, there are several important exemptions which exclude categories of information held by these organisations, or some of their functions, from the coverage of the IPPs. These exemptions are discussed below in the section 'When do the IPPs not apply?'

O.11 The remainder of this section discusses certain categories of organisations in more detail. Some of the categories discussed below are drawn from the above list, while others are classes of organisations about which OVIC frequently receives queries.

Public sector agencies

O.12 The IPPs apply to public sector agencies, which is defined in s 3 of the PDP Act to mean public service bodies or public entities within the meaning of the *Public Administration Act 2004* (Vic).

O.13 Public sector bodies are Departments, Administrative Offices and the Victorian Public Sector Commission.

O.14 Public entities are defined in s 5 of the *Public Administration Act 2004* (Vic). The definition includes certain bodies that are established under an Act or the *Corporations Act 2001* (Cth) or by the Victorian government. Among other requirements, these bodies must have a public function to exercise on behalf of the State, or be wholly owned by the State. Certain types of bodies are expressly excluded from the definition (as listed in s 5(1)(da)-(h) of the *Public Administration Act 2004* (Vic)), such as Parliamentary Committees and Royal Commissions.

Contracted service providers to Victorian government organisations

O.15 Contracted service providers (**CSPs**) may be bound by the IPPs contained in Schedule 1 of the PDP Act where a State contract contains a provision binding the CSP to comply with the IPPs. The CSP is then bound by the IPPs in the same way and to the same extent as the outsourcing public sector organisation.

O.16 If there is no such provision in the State contract, it is the responsibility of the outsourcing public sector organisation to ensure that the CSP upholds the relevant privacy obligations under the PDP Act.

O.17 The IPPs apply to an act or practice of a CSP when:

- there is a State contract between the CSP and the outsourcing government agency;
- that State contract contains a provision binding the CSP to the IPPs, drafted to give effect to s 17(2);

[4] Section 17(2) is a provision which binds the service provider in its contracted obligations to behave as if it were bound by the IPPs and any applicable code of practice in the way that the State party would have been bound.

[5] PDP Act, s 20.

and

- the relevant act or practice was undertaken for the purposes of the State contract.

O.18 A State contract means a contract between an organisation and a CSP under which services are provided by the CSP to the organisation in connection with the performance of the functions of the organisation.

O.19 CSPs to State government are not bound by the Commonwealth *Privacy Act 1988* in relation to their conduct under a State contract. The *Privacy Act 1988* (Cth) expressly gives way to State regulation of organisations providing services under a State contract. However, other activities of the CSP may be regulated by the *Privacy Act 1988* (Cth).

Health service providers

O.20 Victorian public hospitals and health service providers that fall within s 13 of the PDP Act have obligations under the PDP Act in relation to personal information that is not health related. For example, this includes staff records. Private hospitals and health service providers that do not fall within s 13 of the PDP Act are not covered by the PDP Act, unless they are carrying out services under a State contract not related to health. The privacy of health information handled by entities that have access to health information, including both public and private health service providers, is regulated by the *Health Records Act 2001* (Vic). The *Health Records Act 2001* (Vic) is administered by the Health Complaints Commissioner. Private sector health providers may also be regulated under the *Privacy Act 1988* (Cth) which is administered by the Office of the Australian Information Commissioner.

Schools

O.21 State government schools are required to comply with the IPPs. However, independent or denominational schools are not. Typically, independent or denominational schools are subject to the *Privacy Act 1988* (Cth).

Organisations 'established by or under an Act' for a 'public purpose'

O.22 Bodies established or appointed for a public purpose by or under an Act are subject to Part 3 of the PDP Act and the IPPs.[6] This provision refers only to Victorian Acts.[7]

O.23 To determine whether a body was 'established for a public purpose', consider:

- the legislation that establishes the body;
- the organisation's constitution or rules, if they have been referred to in the Act;
- where purposes were multiple or a mix of public and private purposes, whether the dominant purpose of establishing the organisation was public; and
- if more than one dominant purpose, whether one of them was a public purpose. Note 'public purpose' does not just mean 'governmental' purpose – it can be broader and pertains to the people of a community or locality.

[6] PDP Act, ss 13, 20; *Public Administration Act 2004* (Vic) s 5.

[7] *Interpretation of Legislation Act 1984* (Vic) s 38.

When is a public sector organisation responsible for the acts and practices of its agents and employees?

O.24 Section 118 of the PDP Act deems the conduct of an organisation's agents or employees to be the conduct of the organisation itself.

O.25 Where a person has acted within the scope of their actual or apparent authority as an agent or employee of a public sector organisation, an act or practice engaged in by that person, on behalf of the organisation, is taken to be an act or practice of the organisation that employed or engaged them.

O.26 A public sector organisation will therefore be responsible and accountable for a contravention of the IPPs caused by its agent or employee except where:

- the agent or employee acted outside the scope of their duties; or
- the organisation took reasonable precautions and exercised due diligence to avoid the act or practice which caused the contravention of the IPPs.

The agent or employee acted outside the scope of their duties

O.27 Whether an agent or employee acted beyond the scope of their duties will be resolved by reference to principles of agency law. Generally, agents or employees will be acting within their scope of duties where:

- **They were acting within their actual express or implied authority.** This is the authority an organisation has given to its agent or employee in the form of words or writing and any further implied authority that is necessarily incidental to carrying out those express instructions.
- **They were acting within their apparent or ostensible authority.** This is the authority an organisation represents their agent or employee as having, which a third party later relies upon in dealing with the employee or agent.

> **Example – where an employee was acting outside the scope of their duties**
>
> Mr Stewart is a teacher at a State school and a coach of a local soccer team. The local soccer team has no connection to the school. Joe is a student at the school and a player in the soccer team.
>
> Mr Stewart is concerned about Joe's poor performance at soccer and how that could impact the soccer team's ability to play in the finals. Mr Stewart accesses Joe's student record held at the school where he learns that Joe has recently bullied several other students at school. Mr Stewart then uses this information to disqualify Joe from playing in the soccer team.
>
> Mr Stewart accessed Joe's student record for his own benefit as the coach of the local soccer team, not within the scope of his duties as a teacher employed by the school.
>
> Although the school may not be responsible for the use of Joe's personal information by Mr Stewart under IPP 2, they may have failed to take reasonable steps to secure Joe's personal information and therefore be in breach of IPP 4.

Reasonable precautions and due diligence

O.28 It is up to a public sector organisation to demonstrate that it has taken reasonable precautions and

exercised due diligence to avoid its agent or employee from carrying out the act or practice that has caused an interference with privacy.

O.29 This means looking beyond the routine steps a public sector organisation may take in order to demonstrate that it complied with the IPPs. This exception is concerned with the substance of the steps that the organisation has taken rather than only at their existence. That is, it is concerned with the expected and actual impact of the steps it has taken upon the actions of its staff.

O.30 Whether an organisation can demonstrate its actions meet the standard of reasonable precautions and due diligence is to be assessed on a case by case basis. It is an objective test, contextualised by what is reasonable for a public sector organisation that handles personal information of the kind in question.

O.31 It also requires a consideration of whether the organisation could have taken any other steps to prevent the contravention and whether it would be reasonable to expect that such steps would be taken.

O.32 The mere fact that an organisation:

- requires its staff to complete privacy awareness training as part of induction or orientation program;
- requires staff to regularly complete 'refresher' education or training programs;
- has policies or procedures about the handling of personal information which specifically deal with the dispatch of client material by post/ courier and the use of email; and
- has an internal procedure for reporting, containing and escalating known or suspected interferences with privacy;

will not automatically be sufficient to demonstrate that an organisation has taken reasonable precautions and exercised due diligence of the kind contemplated by section 118.

O.33 In considering whether an organisation has taken reasonable steps and exercised due diligence, the following factors are relevant:

- whether the steps taken by an organisation were proportionate to the seriousness and likelihood of harm to the individuals the information is about;
- the availability of alternative steps and the cost and difficulty of implementing them;
- the frequency and nature of privacy training programs for staff; and
- whether policies and procedures are tailored to specific business areas and whether they are used and implemented as part of staff's core work.

> **Example – where an organisation has not take reasonable steps and exercised due diligence**
>
> A Council employee intends to send a group email to several ratepayers who are experiencing financial difficulty. The email provides ratepayers with general information about the support mechanisms available.
>
> The Council employee inadvertently inserts the ratepayers' email addresses into the 'to' instead of the 'bcc' field. This discloses ratepayers' personal information, including: their email address (which in some instances contains their full name) and that they are experiencing financial difficulty.
>
> A review of the incident by the Council reveals that:
>
> - the employee was under time pressures to send the email urgently, this caused them to send the email during a meeting whilst they were multi-tasking and distracted;

- the employee routinely deals with information of that kind and has sent group emails to clients before, without incident;
- the employee has undergone privacy awareness training which is mandatory and assessed for competency. As part of this training, employees are taught to use the 'bcc' instead of the 'to' or 'cc' fields when sending group emails; and
- the Council has a privacy procedure which stipulates that employees should always use 'bcc' instead of the 'to' or 'cc' fields when sending group emails, and that group emails should be peer reviewed before being sent.

Despite these factors, the Council has not taken reasonable steps and exercised due diligence of the kind contemplated by section 118. This is because:

- the risk of harm to individuals affected by the incident is moderate, as it enables other ratepayers to identify potential neighbours experiencing financial difficulty, which could cause embarrassment or distress. This suggests that the steps taken by Council to protect the personal information should have been higher in proportion to the risk of harm;
- whilst Council had a privacy procedure in place which required the peer review of bulk emails before they were sent, which the staff member was familiar with, the privacy procedure could not have been adhered to due to the time pressures impacting upon the employee; and
- Council did not employ any technical solutions to prevent this incident from occurring, even though they were readily available, inexpensive and easy to implement.

When do the IPPs not apply?

Exemptions

O.34 There are limited exemptions applicable to the Victorian government organisations that must comply with the IPPs. The PDP Act does not typically treat particular organisations as exempt. Rather, the PDP Act exempts from protection particular functions of organisations or specific categories of information they hold. Exempt acts and practices, and categories of information, fall outside the protection of some or all of the IPPs. The more significant exemptions are outlined below.

Judicial and quasi-judicial functions of courts and tribunals

O.35 Section 10 of the PDP Act exempts courts and tribunals from compliance with the IPPs or any protective data security standard in respect of the exercise of judicial or quasi-judicial functions. The IPPs will still apply to personal information collected for other court and tribunal functions, such as the maintenance of staff records, or general administrative matters.

O.36 'Quasi-judicial' means 'court like'. It includes the actions of non-judicial bodies, such as administrative agencies, exercising their functions and powers in a judicial manner. In deciding whether an action or proceeding is 'quasi-judicial', various factors may be taken into account. These include whether a proceeding's purpose is to make a determination or finding concerning a matter, the truth of which is of public concern.

O.37 A statute which establishes a tribunal and regulates its procedures helps to determine whether a government body is a 'tribunal'. A body does not need to be called a tribunal. Relevant factors in determining whether or not a body is a tribunal include whether provision is made for its proceedings, for the calling of witnesses and receiving evidence on oath, for public hearings, legal representation, and immunity of decision makers from suit. In addition, the relevant statute will often describe the tribunal's initiating mechanisms and the legal consequences of its determinations.

O.38 A court registry's handling of its case records and other documents filed by parties for the purposes

of proceedings are likely to be matters *which relate to* judicial functions and therefore be exempt from obligations under the PDP Act.

O.39 'Judicial power' was described by the Victorian Supreme Court in *R v Debono*:[8]

> 'Judicial power involves, as a general rule, a decision settling for the future a question between identified parties as to the existence of a right or an obligation. In this regard, the process is generally an inquiry concerning the law as it is and the facts as they are, followed by an application of the law as determined to the facts as determined.'

O.40 In *Harrison v VBA*,[9] VCAT found that the then Building Practitioners Board (**BPB**) was a tribunal that had a quasi-judicial function because it:

- had an inquiry function concerning facts and law;
- applied the law; and
- made a determination affecting the obligations and rights of the parties involved.

O.41 VCAT also found that even though the employees exercising the quasi-judicial function worked for a related body (not the BPB), it was deemed that the employees were exercising the functions of the BPB.

Parliamentary Committees

O.42 Section 11 of the PDP Act provides that nothing in the PDP Act, the IPPs or a protective data security standard applies in respect of the collection, holding, management, use, disclosure or transfer of personal information by a Parliamentary Committee in the course of carrying out its functions.

Royal Commissions

O.43 Section 10A of the PDP Act provides that nothing in the PDP Act, the IPPs or any data security standard applies in respect of the collection, holding, management, use, disclosure or transfer of information by a Royal Commission, a Board of Inquiry or a Formal Review for the purposes of, or in connection with, the performance of its functions.

Personal information in documents subject to the *Freedom of Information Act*

O.44 Section 14 states that nothing in IPP 6 applies to personal information contained in documents subject to the *Freedom of Information Act 1982* (Vic) (**FOI Act**). Organisations subject to the FOI Act therefore do not need to comply with IPP 6.

O.45 For more information on the relationship between IPP 6 and the FOI Act, see the IPP 6 chapter of these Guidelines.

Law enforcement activities

O.46 Section 15 of the PDP Act provides that a law enforcement agency does not have to comply with IPPs 1.3 to 1.5, 2.1, 6.1 to 6.8, 7.1 to 7.4, 9.1 or 10.1 in certain circumstances. The law enforcement agency will not need to comply with these IPPs if it believes, on reasonable grounds, that non-compliance is reasonably necessary:

---

[8] *R v Debono* [2012] VSC 350 [51], citing *R v Trade Practices Tribunal; Ex parte Tasmanian Breweries Pty Ltd* (1970) 123 CLR 361, 374.

[9] *Harrison v Victorian Building Authority* (Human Rights) [2015] VCAT 1791 [23].

a. for its own, or another law enforcement agency's enforcement functions;
b. for the enforcement of laws relating to the confiscation of the proceeds of crime;
c. in connection with proceedings commenced in a court or tribunal; or
d. in the case of Victoria Police, for the purposes of its community policing functions.

O.47 Certain bodies are defined in s 3 of the PDP Act as 'law enforcement agencies'. They include, for example, a State police force and the Australian Federal Police, the Australian Crime Commission, the Commissioner of Corrections and the Business Licensing Authority. Also included in the definition are agencies whose function it is to:

a. prevent, detect, investigate, or prosecute criminal offences or breaches of a law imposing a penalty or sanction for a breach
b. manage property seized under laws relating to confiscation of proceeds of crime;
c. execute or implement an order or decision of a court or tribunal; or
d. protect the public revenue under a law administered by the law enforcement agency.

O.48 Organisations seeking to rely on this exemption must believe, with a reasonable basis for that belief, that non-compliance with the IPPs listed in s 15 is necessary in the particular circumstances. This means that law enforcement agencies do need to consider and adhere to the IPPs, except where doing so is incompatible with their law enforcement functions.

O.49 In *Zeqaj v Victoria Police* (Human Rights) [2018] VCAT 1733, Member Dea said:

> 'the belief [that noncompliance is necessary] must not only be that the duty or task must be undertaken but that, in order to perform that duty or task, it is necessary not to first comply with the IPPs which would otherwise apply. The belief the noncompliance is necessary is linked not to the action [the law enforcement agency] intends to take, but to the IPPs would otherwise apply …
>
> … in order for section 15 of the Privacy Act to apply, there must be evidence of a belief of the kind referred to having been formed'.[10]

O.50 For more information about this case, see Case Study 2S (under the 'Disclosure to relevant persons and authorities' section) in the IPP 2 chapter of these Guidelines.

Family Violence Protection Act

O.51 Section 15A of the PDP Act exempts specified entities from complying with certain IPPs for the purposes of information sharing under the *Family Violence Protection Act 2008* (Vic) (**FVP Act**).

O.52 Information Sharing Entities (**ISEs**)[11] and the Central Information Point (**CIP**)[12] are exempt from complying with IPPs 1.4 and 1.5 when collecting personal information for the purposes of Part 5A of the FVP Act. Authorised Hub entities are not required to comply with IPPs 1.3, 1.4 and 1.5 when collecting personal information for the purposes of Part 5B of the FVP Act.

O.53 The CIP is expressly exempt from IPP 6, meaning the CIP is not required to provide access to or correct personal information about an individual that the CIP has collected for the purposes of Part

[10] *Zeqaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018) [81]-[83].

[11] An ISE is defined under s 144D of the *Family Violence Protection Act 2008* (Vic) (**FVP Act**) to be a person or body prescribed, or a class of person or body prescribed, to be an information sharing entity.

[12] The CIP is a secure statewide service that collates information relevant to family violence risk assessment and risk management.

5A of the FVP Act. (Part 5A relates to information sharing.) 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.

O.54 An ISE may refuse access to information under IPP 6 where a family violence risk has been established, if the individual making the request is a perpetrator or alleged perpetrator.[13] This provides ISEs with a greater ability to ensure victim survivors are not unduly exposed to increased risk from perpetrators accessing information about them.[14] See IPP 6.7 for more information about providing reasons for denying access or refusal to correct personal information.

O.55 In addition to the above exceptions from the IPPs under the scheme, the *Victorian Data Sharing Act 2017* (Vic) 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.

O.56 For more information about information sharing under the FVP Act, refer to OVIC's *Family violence information sharing scheme and privacy law FAQs*.

Child Wellbeing & Safety Act

O.57 Section 15B of the PDP Act exempts specified entities from complying with certain IPPs for the purposes of information sharing under the *Child Wellbeing and Safety Act 2005* (Vic) (**CWS Act**).

O.58 ISEs are exempt from collecting information directly from the relevant individual under IPP 1.4 for the purposes of Part 6A of the CWS Act, which relates to information sharing. Child Link users and the Secretary to the Department of Education and Training are also exempt from IPP 1.4 when collecting personal information for the purposes of Part 7A of the CWS Act, which relates to the Child Link Register.[15] This means these entities are not required to collect personal information about a person directly from them, and can instead collect the information from another ISE.

O.59 ISEs are exempt from notifying individuals when personal information has been collected from another person under IPP 1.5 when collecting personal information for the purposes of Part 6A of the CWS Act, to the extent that compliance with IPP 1.5 would be contrary to the promotion of the wellbeing or safety of a child (to whom the information relates).[16] This exemption removes the obligation on ISEs to take reasonable steps to notify individuals that their personal information has been collected from another ISE.

O.60 Child Link users or the Secretary to the Department of Education and Training are exempt from IPP

[13] FVP Act, s 144QA.

[14] 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.

[15] See s 46B of the CWS Act for further information about the Child Link Register. A Child Link User is a person who is authorised to access the Child Link Register as specified in Part 7A of the CWS Act.

[16] PDP Act, s 15B(2).

1.5 where personal information is collected for the purposes of Part 7A of the CWS Act.[17] This exemption also removes the requirement of Child Link users or the Secretary to notify individuals of indirect collection, where providing notice would be contrary to the promotion of a child's wellbeing or safety.

O.61 ISEs may refuse to disclose confidential information under IPP 6, where an individual has requested access to their personal information, if they believe on reasonable grounds that access to the information would result in an increased safety risk to children.[18] See IPP 6.7 for more information about providing reasons for denying access or refusal to correct personal information.

O.62 ISEs are exempt from IPP 10.1 when collecting sensitive information under Part 6A of the CWS Act. Similarly, Child Link users or the Secretary to the Department of Education and Training are also exempt from IPP 10.1 when collecting sensitive information under Part 7A of the CWS Act.[19] This means that sensitive information can be collected despite the restrictions under IPP 10.1.

O.63 When sharing information under Parts 6A and 7A of the CWS Act, the IPPs will not apply to the collection, use or disclosure of personal, sensitive or health information by an ISE, Child Link user or the Secretary to the Department of Education and Training, to the extent that the IPPs require the consent of the person to whom the information relates.[20] In practice, ISEs, Child Link users or the Secretary will not be required to obtain consent from any person prior to collecting information, including sensitive information under IPP 10.1, if they are sharing in accordance with the scheme.

O.64 It is important to note that the notice requirements under IPP 1.3 continues to apply to ISEs. When an ISE is collecting information directly from an individual, they are required to take reasonable steps to make the individual aware of particular matters at or before the time the information is collected, or as soon as practicable after.

O.65 For more information about information sharing under the CWS Act, refer to OVIC's *Child information sharing scheme and privacy law FAQs*.

Health Services Act 'quality and safety' purposes

O.66 Section 15C of the PDP Act contains exemptions from complying with certain IPPs for the purposes of information sharing under Part 6B of the *Health Services Act 1988* (Vic) (**HSA**).

O.67 The purposes for which information can be shared under Part 6B of the HSA include:

- collecting and analysing information relating to the quality and safety of health service entities;[21]
- monitoring and reviewing the quality and safety of health service entities and associated risks;
- reporting the performance of a health service entity;
- reporting a risk to an individual or community associated with the performance of a health service entity; and

[17] PDP Act, s 15B(3).

[18] CWS Act, s 41ZF.

[19] PDP Act, s 15B(4).

[20] PDP Act, s 15B(5).

[21] A 'health service entity' is defined under s 134V of the HAS as a public health service, public hospital, multipurpose service, denominational hospital, private hospital, day procedure centre, ambulance service, non-emergency patient transport service within the meaning of the *Non-Emergency Patient Transport Act 2003* (Vic) or a prescribed entity that provides a health service.

- incident and performance reporting in relation to a health service entity.

O.68 The Secretary to the Department of Health and Human Service, quality and safety bodies[22], health service entities and special advisers[23] (collectively **Part 6B entities**) are exempt from complying with:

- IPP 1.4 (the requirement to collect personal information directly from the person it relates to);
- IPP 1.5 (the requirement to tell an individual if personal information about them is collected from a third party); and
- all IPPs that require an individual to consent to the collection of their personal information.

O.69 This means Part 6B entities are not required to collect personal information directly from the individual the information relates to, or provide a collection notice to that individual.

> **Example**
>
> Safer Care Victoria is investigating several failed high-risk procedures which occurred at Hospital A. In order to compare the outcomes, Safer Care Victoria requires the names and specialities of clinicians involved in the high-risk procedures. In collecting the personal information of the clinicians from Hospital A, Safer Care Victoria is exempt from having to collect the personal information directly from clinicians (IPP 1.4) and providing the clinicians with a collection notice (IPP 1.5).

O.70 In addition, Part 6B entities are not required to obtain an individual's consent when assigning a unique identifier to the individual (IPP 7.1), transferring the personal information to an entity who resides outside of Victoria (IPP 9.1) or when collecting sensitive information (IPP 10). However, as s 15C only provides for the displacement of the requirement to obtain consent, Part 6B entities will still need to comply with the other operative requirements of the relevant IPP.

O.71 For more information about information sharing under Part 6B of the HSA, refer to OVIC's *Protecting privacy while sharing information under the new Part 6B of the Health Services Act 1988: Guidance for practitioners.*

Publicly-available information

O.72 Section 12 of the PDP Act provides that nothing in the Act, the IPPs or a protective data security standard applies to personal information contained in a document that is:

- a generally available publication;
- kept in a library, gallery or museum for the purposes of reference, study or exhibition;
- a public record under the control of the Keeper of Public Records and available for public inspection in accordance with the *Public Records Act 1973* (Vic); or
- archives within the meaning of the *Copyright Act 1968* (Cth).

O.73 A generally available publication is defined in s 3 of the PDP Act as 'a publication (whether in paper or electronic form) that is generally available to members of the public and includes information held on a public register'. Whether information that is publicly-available can be considered to be part of a 'generally available publication' will depend upon the context in which the information appears. In

[22] A 'quality and safety body' is defined under s 134V of the HSA as an entity prescribed with a function relating to quality and safety of health services entities.
[23] A 'special adviser' is defined under s 134V of the HSA as an entity appointed as a special adviser by the Secretary to the DHHS or quality and safety body under s 134Z of the HSA.

the case of online information, the following factors can help determine whether information is in a 'generally available publication':

- the nature of the information;
- the prominence of the web page on which it is located;
- the likelihood of access by members of the public; and
- the steps needed to obtain that access.[24]

O.74 In *Jurecek v Director, Transport Safety Victoria*,[25] the Supreme Court of Victoria found that an individual's Facebook 'chats' and 'posts' did not constitute a 'generally available publication', even though they could be accessed via Facebook by anybody. Justice Bell said:

> 'That information, otherwise personal, might be accessible on some Facebook by anybody does not necessarily mean that the information is a generally available publication; equally, that information, otherwise personal, might be accessible somewhere on the Internet by anyone does not necessarily mean that the information is a generally available publication …
>
> Mere publication of information on Facebook or the Internet does not, in my view, necessarily make it a 'generally available publication'. [26]

Examples of 'generally available publications'

Sentencing remarks published on Austlii's website

O.75 In *DNV v Department of Health and Human Services*[27] the Tribunal considered whether sentencing remarks published on Austlii's website (that included the complainant's name) were exempt from the PDP Act. The Tribunal found that the name was contained in a 'generally available publication' at the time the complainant's information was used and disclosed by Department. This finding was made despite subsequent pseudonymisation of the complainant's name.

Public registers

O.76 Public registers will usually be regarded as a 'generally available publication',[28] and subject to this exemption. However, s 12 does not *wholly* exclude information contained in public registers from privacy protection. Section 20(2) provides that public sector agencies and councils administering public registers must, *so far as is reasonably practicable*, not do an act or engage in a practice that would contravene an IPP in respect of any personal information handled. Essentially, the PDP Act's intention is for the IPPs to apply 'so far as is reasonably practicable' to personal information held on public registers. Such information is collected, often compulsorily, and held for particular purposes. The PDP Act recognises that while public register information should be able to be used for the legitimate purposes for which it is collected, unrelated uses (which are not permitted by the IPPs) are generally treated as interferences with privacy.

---

[24] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [84] (Bell J). This case was specifically concerned with information on a website (Facebook).

[25] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285.

[26] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 [84], [93] (Bell J).

[27] *DNV v Department of Health and Human Services* (Human Rights) [2017] VCAT 1569.

[28] *Taylor v Victorian Institute of Teaching* (Human Rights) [2013] VCAT 1290.

Flexibility mechanisms

O.77 The PDP Act provides a number of mechanisms allowing organisations to depart from the IPPs, or to clarify their operation. The relevant mechanisms under the PDP Act are:

- Public Interest Determinations (**PID**);
- Temporary Public Interest Determinations (**TPID**);
- Information Usage Arrangements (**IUA**); and
- certification of an act or practice.

Public Interest Determination and Temporary Public Interest Determinations

O.78 A Public Interest Determination (**PID**) and a Temporary Public Interest Determination (**TPID**) are a written determination by the Information Commissioner, which permits an act or practice that would otherwise have been a breach of the IPPs, while the PID or TPID is in place.

Information Usage Agreements

O.79 Information Usage Arrangements (**IUAs**) can modify the application of IPPs or codes of practice or provide that the practice does not need to comply with them (except IPP 4 and IPP 6). IUAs can also permit handling personal information for the purposes of an information handling provision.

O.80 It is anticipated that organisations will mostly seek approval of IUAs to allow personal information to be used or disclosed for a purpose or to entities that were not anticipated at the time the information was collected.

Certifications

O.81 The Information Commissioner can certify that an act or practice is consistent with:

- an Information Privacy Principle; or
- an approved code of practice; or
- an information handling provision.[29]

O.82 Certification of an act or practice means the organisation that does an act or engages in a practice in good faith in accordance with the certification does not contravene the relevant IPP, approved code of practice or information handling provision.[30]

More information

O.83 For more detailed information on flexibility mechanisms, refer to the *Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arrangements and Certification*.

Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond

[29] PDP Act, s 55.

[30] PDP Act, s 55(4).

to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

Version control table

Version	Description	Date published
Overview 2020	Addition of commentary on s 15C and s 118.	3 December 2020
Overview 2019.B	Edits following consultation.	14 November 2019
Overview 2019.A	Consultation draft.	1 August 2019
Overview (2011)	2011 pdf version.	2011