Office of the Victorian Information Commissioner

IPP 2 – Use and Disclosure

IPP 2 – Use and Disclosure

On this page

2.1 The basic rule of IPP 2.1 is relatively straightforward: use and disclose personal information only for the purpose for which it was collected (the 'primary purpose').

2.2 However, IPP 2 allows the use and disclosure of personal information in certain circumstances for other purposes ('secondary purposes').

2.3 IPP 2 contains eight other instances where use or disclosure may be permitted for a secondary purpose. These are contained in IPPs 2.1(a)–(h). Seven of these envisage use or disclosure without consent.

What is a 'use' or 'disclosure?'

2.4 The terms 'use' and 'disclosure' are not defined in the PDP Act.

2.5 The Macquarie Australian Dictionary defines 'use' as 'employ for some purpose'. Examples of uses of personal information by an organisation include:

- a staff member of the organisation accessing and reading the personal information;
- the organisation making a decision based on the personal information;
- the organisation passing the personal information from one part of the organisation to another; and
- unauthorised access to the personal information by an employee of the entity.

2.6 The term 'disclose' takes its ordinary dictionary meaning: 'opening something up to view or revealing it'. An organisation 'discloses' information where it releases the information out of its effective control and into the control of another organisation or person. The release may be a proactive release or publication, a release in response to a specific request, or an accidental or unauthorised release.

2.7 Accidental or unauthorised disclosures may also breach IPP 4 (Data Security).

Verbal disclosure of recorded information

2.8 As noted in Key Concepts, personal information must be 'recorded in any form'.[1]

2.9 However, IPP 2 applies to all disclosures of recorded personal information, no matter how the disclosure occurs. For example, IPP 2 applies to verbal disclosures of personal information that also exists in a recorded form.

Disclosure by allowing others to view information

2.10 Personal information can be disclosed even though it remains in the possession or control of its original collector. For example, if a person from outside an organisation is permitted to read information held by an organisation on a computer screen, then the organisation has disclosed the information to the person.

Intra-organisation uses and disclosures

2.11 Internal information sharing within the same organisation or legal entity is considered to be 'use' of information. In contrast, sharing information with another legal entity is 'disclosure'. However, the legal personality of an organisation can be confusing because many Victorian public sector

[1] PDP Act, s 3 (definition of 'personal information').

organisations are closely related to each other or may fall under the same portfolio department. Departmental portfolios are commonly comprised of distinct business units, statutory agencies and independent statutory offices. For example, a Department may have various business units, panels, commissions, boards and other entities carrying out many functions in diverse areas.

2.12 These individual entities may be separate 'organisations' under s 13 of the PDP Act. They will have different functions, which will impact on the types of personal information collected. These separate entities may also have other legal authorisations to collect personal information, for example, under their enabling legislation, and obligations of confidentiality that impact the entity's authority to collect or disclose information.

2.13 Complicated organisational structures in the public service can make it difficult to determine whether a particular action is an internal use or external disclosure. In practice, the distinction is not significant because often the same requirements attach to both use and disclosure under IPP 2.

2.14 A disclosure by one body or entity will constitute a collection by the recipient body. Organisations, and entities within a departmental portfolio, should ensure they comply with both IPP 1 (Collection) and IPP 2 (Use and Disclosure) when they share personal information (while keeping in mind their obligations under other relevant IPPs).

IPP 2.1: Primary purpose

2.15 IPP 2.1 permits use and disclosure for the primary purpose for which the personal information was collected. This is the 'primary purpose'. The purpose for which information is collected can be inferred from or implicit in the circumstances of collection.[2] Therefore, IPP 2.1 is linked to collection notices (issued under IPP 1.3), as organisations should have already explained the primary purpose of collection to the individual. This means organisations need to consider and define the specific function to activity for which they are collecting the information.

2.16 In *Ng v Department of Education* [2005] VCAT 1054 at [88]-[89], VCAT defined 'purpose' narrowly as 'synonymous with the intent' of collection and avoided a purely objective analysis of purpose as this will often be too wide. This means the primary purpose is narrow. In contrast, a number of recent VCAT cases listed below have shown defined the primary purpose widely. Further discussion of the meaning of 'purpose' is in Key Concepts. A narrow definition of purpose best protects individuals' privacy.

2.17 Inadvertent disclosures may still be for a 'purpose'. For example, disclosure might be for a purpose, but the information is sent to the wrong person. The inadvertent or accidental disclosure is still for that original purpose, despite the error.[3]

Identifying the primary purpose

2.18 A statute might set a broad primary purpose, however, organisations themselves should avoid this because it will increase the likelihood of use and disclosure being found to be outside a more narrowly construed primary purpose. This will breach IPP 2.1, unless an exception applies. The following examples may help organisations to define and describe the primary purpose of collection.

- In *Harrison v Victorian Building Authority* (Human Rights) [2017] VCAT 108 [114], the primary

[2] *Little v Melbourne City Council* (General) (2006) VCAT 2190 [20], [21]-[23].

[3] *TSJ v Department of Health and Human Services* (Human Rights) [2016] VCAT 687 (11 May 2016) [19].

purpose was the administration of complaints. The disputed disclosure fell within this primary purpose because the statutory complaints process in the *Building Act 1993* (Vic) made it clear to applicants their information would be disclosed.

- In *Zeqaj v Victoria Police* (Human Rights) [2018] VCAT 1733 [91], the use of personal information to assess a firearms licence was within Victoria Police's primary purpose of collection: to preserve the peace, protect life and property, prevent the commission of offences and detect and apprehend offenders. This broad purpose was taken from the duties of police officers under the *Victoria Police Act 2013* (Vic).

- In *Taylor v Victorian Institute of Teaching* (Human Rights) [2013] VCAT 1290 [137] to determine the primary purpose, VCAT considered the respondent's privacy policy and express functions under the relevant Act. VCAT considered the primary purpose of collection was to undertake statutory functions, which included regulating the teaching profession, maintaining standards and investigating the conduct of teachers.

2.19 This list shows the primary purpose for collection will vary in breadth and generality according to the circumstances of collection, use or disclosure. OVIC suggests organisations define the primary purpose of collection of personal information narrowly.

Compulsorily acquired information

2.20 Where an organisation compulsorily acquires personal information, the purposes for which it can use and disclose that information will be more limited than if the information was obtained voluntarily. This is for two reasons. First, the scope of the power used to compulsorily acquire the information will limit the scope of the primary purpose of collection. Second, the fact that the information was compulsorily acquired may impose an obligation of confidence upon the organisation, in accordance with the principle discussed in *Johns v Australian Securities Commission* (1993) 178 CLR 408. In this case, Justice Brennan of the High Court of Australia said:

> *When a power to require disclosure of information is conferred for a particular purpose, the extent of dissemination or use of the information disclosed must itself be limited by the purpose for which the power was conferred. In other words, the purpose for which a power to require disclosure of information is conferred limits the purpose for which the information disclosed can lawfully be disseminated or used…*
>
> *A statute which confers a power to obtain information for a purpose defines, expressly or impliedly, the purpose for which the information when obtained can be used or disclosed. The statute imposes on the person who obtains information in exercise of the power a duty not to disclose the information obtained except for that purpose. If it were otherwise, the definition of the particular purpose would impose no limit on the use or disclosure of the information. The person obtaining information in exercise of such a statutory power must therefore treat the information obtained as confidential whether or not the information is otherwise of a confidential nature. Where and so far as a duty of non-disclosure or non-use is imposed by the statute, the duty is closely analogous to a duty imposed by equity on a person who receives information of a confidential nature in circumstances importing a duty of confidence…*
>
> *It is therefore important to ascertain the purposes for which such information can be*

legitimately used or disclosed.[4]

2.21 This case concerned the disclosure of transcripts of evidence by the former Australian Securities Commission (**ASC**) to the Royal Commission into the collapse of the Tricontinental group of companies. The transcripts of Johns' evidence (the managing director of the companies at the time) had been acquired through the compulsory examination powers of the ASC and were subject to confidentiality obligations and strict limitations around use and disclosure. The ASC permitted the Royal Commission to use the material in public hearings, which were then reported by the media.

2.22 Johns successfully argued that he had been denied natural justice by the ASC for not being provided an opportunity to be heard before they allowed the confidential material to be publicly disseminated, so as to prejudice his rights or interests. Public disclosure could prejudice Johns' personal reputation and encroach on his right to maintain silence about the matters being investigated by the ASC. The High Court of Australia held that the ASC's decision to disclose the transcripts to the Royal Commission for use in public hearings was therefore invalid.

2.23 Where an organisation has compelled the provision of information, it should be cautious about disclosing that information for any other purpose.

2.24 There are many situations where individuals are compelled to provide their information in order to obtain a benefit, exercise a right, or comply with a legal obligation. Examples include:

- obtaining a driver's licence or registering a motor vehicle;
- registering a pet cat or dog;
- planning to renovate or build a house, or objecting to a planning proposal;
- applying for public housing;
- practising as a professional (for example, as a teacher, lawyer or doctor);
- seeking a licence to operate a childcare centre;
- working in certain child-related areas;
- voting at state and local government elections; or
- complying with notices to produce documents or give evidence.

2.25 Organisations should carefully examine any laws underpinning the compulsory collection of information to ensure any subsequent use or disclosure of that information is permitted.

IPP 2.1(a): Reasonably expected related secondary purposes

2.26 Under IPP 2.1(a), an organisation can use and disclose personal information for a related secondary purpose, if the individual the information is about would reasonably expect the organisation to do so.

Determining whether a proposed use or disclosure is authorised under IPP 2.1(a)

2.27 The secondary purposes for use and disclosure must be related to the primary purpose of collection and consistent with what an individual would reasonably expect. In the case of sensitive information, the secondary purpose must be directly related.

2.28 This is a two-part test:

[4] *Johns v Australian Securities Commission* (1993) 178 CLR 408 [14]-[15]. See also, [3] (Dawson J), [1] (Gaudron J), [9] (McHugh J).

- Is the **secondary purpose related** (or directly related) to the primary purpose?
- Would the individual whose information was collected **reasonably expect** the use or disclosure?

Related secondary purposes

2.29 The secondary purpose for which the information is used or disclosed has to be connected to or associated with the primary purpose. It must **relate** to the primary purpose for which it was collected. If sensitive information is involved, the secondary purpose has to be directly related to the primary purpose. VCAT has said the link between the primary and secondary purposes must be 'clear, undeniable and inextricable'.[5]

2.30 The Explanatory Memorandum to the PDP Act suggests that a reasonably expected secondary use would be where information collected in delivering a government service is subsequently used to manage, evaluate or improve that particular service. So, quality assurance, program evaluation and development are likely to be regarded as reasonably expected secondary purposes. The Explanatory Memorandum says:

> *[Organisations] are entitled to use or disclose personal information for a secondary purpose where it is related to the primary purpose of collection and the use or disclosure is within the reasonable expectations of the individual. This would be the case, for example, where the information was used to manage, evaluate or improve particular government services in relation to which the information was originally collected. Secondary uses or disclosures are otherwise permitted in cases where there is a strong public interest in doing so.*[6]

2.31 In *Ng v Department of Education* [2005] VCAT 1054, the Department installed a CCTV camera in the computer room of a school to minimise the risk of vandalism and to monitor student use of the computers. The CCTV footage was subsequently used during an investigation into the teacher's work performance in the classroom. In that case, VCAT found the purpose of installing the CCTV camera was not the broad purpose of taking visual recordings of any 'relevant incident' that may need to be investigated, but the specific purpose of collecting information about student misbehaviour and inappropriate conduct. However, use of the CCTV footage to assess the teacher's performance in managing inappropriate student behaviour was a secondary purpose because it 'clearly related to monitoring the inappropriate behaviour itself'.[7]

2.32 Examples of related secondary purposes, found to be within the reasonable expectations of the person involved include:

- the use of personal information by local councils for fire and flood protection. Local councils may collect information from ratepayers in relation to owners' properties. The primary purpose of collection may be to make decisions about amenities, value, uses and upkeep of those properties. However, disclosure of this information to a relevant authority for the secondary purpose of safety against bushfire, flood or extreme weather would be a related and reasonably expected secondary purpose.
- the secondary use by police of firearm licence holders' fingerprints in the investigation of

[5] *Ng v Department of Education* [2005] VCAT 1054 (6 June 2005) [94].

[6] Explanatory Memorandum, Privacy and Data Protection Bill 2014 (Vic), 34.

[7] *Ng v Department of Education* [2005] VCAT 1054 [89]-[94].

crime.[8]

- the disclosure of a tertiary student's contact details to a debt collector after the student incurred a debt for a course. This was related to the primary purpose of collection, that is, the enrolment of fee-paying students.[9]

2.33 In some cases, use or disclosure will not be related, despite what may seem at first to be an apparent link between the primary purpose and the disclosure. For example, in *Duggan v Moira Shire Council* (Unreported, VCAT, Preuss SM, 11 October 2004) [35], VCAT found the primary purpose of collecting the identity of a person who found a dog, was not related to the secondary purpose of informing the grateful owner of the finder's details so that the owner could thank the finder:

> *I am unable to accept the submission that the secondary purpose was related to the primary purpose. The primary purpose of collection was to enable the Council to make contact with the (finder) to collect the dog, and if there were any difficulties in so doing, to get further particulars of the dog's whereabouts. I am not satisfied that the disclosure of the (finder's) name to (the owner) was related to this purpose*.

Reasonably expected

2.34 The second part of the test for IPP 2.1(a) is if the individual whose information was collected reasonably expect the use or disclosure.

2.35 For a use or disclosure to be 'reasonably expected', it is necessary to ask what an ordinary person in the position of the person who the information is about would consider reasonable. This is an objective test. It is the reasonable expectation of an ordinary person, who is not necessarily expert in the workings of government, that is to be considered in the particular circumstances.

2.36 The expectations of the actual individual involved are a consideration, but they are not determinative.

Case Study 2A: Referral of ministerial correspondence reasonably expected[10]

A Minister disclosed personal information about a complainant to the organisation which was the subject of the complaint.

The Commissioner considered the disclosure to be part of the primary purpose insofar as a Minister would typically refer matters to those with the requisite responsibility or capacity to assist on a matter. The Commissioner said that even if such a disclosure was not for the primary purpose, it was for a reasonably expected secondary purpose related to the primary purpose.

The Commissioner reasoned that an ordinary person, although not expert in government administration, would reasonably expect that the Minister and his or her personal staff do not themselves deal with the detail of complaints and enquiries from the public. Rather, a person would reasonably expect that the Minister and his or her staff would refer the complaint (and the complainant's details) to those who can and should deal with them.

[8] *Complainant AB v Victoria Police* [2006] VPrivCmr 3.

[9] *Complainant M v Tertiary Institution* [2004] VPriv Cmr 7.

[10] *Complainant D v Minister* [2003] VPrivCmr 4.

2.37 A secondary use or disclosure might be reasonably expected where that use or disclosure is 'inextricably linked' to the primary purpose of collection. In *Ng v Department of Education*, VCAT found that:

> *(T)he inextricable link between inappropriate behaviour by students and the quality of teachers' management of that behaviour is so close as to render it reasonably foreseeable by a reasonable teacher that footage taken for the one purpose should be used for the other.*[11]

Factors affecting reasonableness of expectation

2.38 Whether an ordinary person would reasonably expect the use or disclosure will depend upon the circumstances of each case. A number of factors can influence this assessment, including:

- the manner in which the information was given to the organisation;
- the notice provided to the individual upon collection;
- the sensitivity of the personal information;
- the nature of the organisation;
- the actions of the individual in question; or
- the individual's expressed expectations.

The manner in which the information was given to the organisation

2.39 The context in which an organisation collects the personal information from an individual affects the reasonableness of expectations of use and disclosure.

Case Study 2B: Disclosure of petitioners' details reasonably expected[12]

A member of the public organised a petition and sent it to his local council. The Council invited him to attend the meeting in which it was tabled for discussion. The Council later posted the petition on its website as part of the minutes of the meeting. The petitioner was concerned that his personal details (name and address) were available on the petition and thus on the website.

In the Commissioner's view, the primary purpose for which the Council collected the personal information contained in the petition was to facilitate the democratic process in government decision-making.

The Council had discussed the petition at an ordinary meeting that was open to members of the public. Moreover, councils, like all government bodies, have a duty to be accountable and, where possible, transparent to the public. Accordingly, the minuting of the petition and its discussion, along with any arising decisions by Council were all related

[11] *Ng v Department of Education* [2005] VCAT 1054 [95].

[12] *Complainant H v Local Council* [2004] VPrivCmr 2 (26 February 2004).

secondary purposes for which it was collected.

The assessment of whether a related secondary purpose is reasonably expected is an objective one: would an ordinary person, although not expert in government administration, reasonably expect that any personal information they put on a petition, circulated through the community and tabled at a public meeting, would ultimately be disclosed?

The Commissioner considered that a person would reasonably expect such a disclosure.

The notice provided to the individual upon collection

2.40 Collection notices can outline the secondary purposes for which the information is to be used or disclosed (see IPP 1.3). Collection notices can help create an expectation that information is to be used for related secondary purposes. However, further communication with an individual may be required to establish that the secondary use is 'reasonably' expected. For example, a secondary use or disclosure that breaches an undertaking of confidentiality cannot be said to be 'reasonably' expected. Collection notices cannot be used to override other existing legal obligations.

2.41 Reasonableness also requires the related secondary use or disclosure is proper and fair, and generally not incompatible with the primary purpose of collection. Organisations that give notice of their intention to use or disclose information in a way that is different to what a person might reasonably expect may find that individuals will not want to transact with the organisation. Similarly, individuals may not want to provide complete and accurate information to organisations.

The sensitivity of the personal information

2.42 Later disclosures of information may be influenced by the manner in which the information was received by the organisation or whether the information is sensitive or delicate information.

2.43 For example, in *Complainant H v Local Council* [2004] VPrivCmr 2 (see Case Study 2B above), in addition to finding the disclosure in council minutes of petitioners' details was in accordance with the primary purpose of collection, the former Privacy Commissioner found the circumstances in which the information was gathered and presented to Council also created a reasonable expectation that it would be publicly disclosed. However, the Privacy Commissioner cautioned that there may be cases where disclosure would not be appropriate because that disclosure would reveal sensitive or delicate information.

> *An ordinary person, although not expert in government administration, would reasonably expect that to put their name to a petition that is to be circulated throughout the community to gather more signatures, with a view to having the petition tabled at a public meeting, would result in the disclosure of any personal information they elect to put on the petition.*
>
> *Only in the rarest of circumstances, such as a petition by persons who all have a particular illness petitioning for better health services, will disclosure not be appropriate. In the example given of illness, to disclose would reveal more about a person than just their name and address. In such cases it might be appropriate to keep private the actual names and addresses while*

disclosing the subject matter of the petition itself.[13]

The nature of the organisation

2.44 The type of organisation using and disclosing the personal information will affect how reasonable it is to expect the particular use or disclosure. In Case Study 2B above, the organisation publishing the petition online was a local council, an organisation that facilitates public discussion of various matters important to the community. For example, the reasonableness of the disclosure in Case Study 2B can be contrasted with the publication of a petition by a private organisation that does not have such a role in the democratic process.

2.45 The extent to which personal information might reasonably be expected to be disclosed within an organisation will also be influenced by matters such as the size of the organisation and the functions of the individuals within the organisation (affecting their 'need to know'). For example, in *Complainant Q v Contracted Service Provider to a Department* [2005] VPrivCmr 3, the former Privacy Commissioner accepted it was reasonably expected that a Human Resources Manager could pass on the outcomes of a criminal record check for a job applicant to two senior staff members with responsibility for supervision and management of the person's work. A person would reasonably expect that the information would not flow outside the organisation, or to people within the organisation who did not have a 'need to know.'

The actions of the individual in question

2.46 Individuals that disclose their own information in a public forum, for example, by talking to the media about a complaint they made about a public sector organisation, should reasonably expect that the public sector organisation will respond to media inquiries and may, in responding, disclose the person's information in a proportionate manner. In *Complainant Y v The Department* [2005] VPrivCmr 7 the former Privacy Commissioner stated:

> *I consider that an individual who speaks willingly to a journalist (whom s/he knows writes articles for publication), about matters that are to be the subject of a public tribunal process, would reasonably expect that the organisation complained about may also respond in public… An organisation may communicate with a number of media organisations to ensure its reputation and interests are protected, if each has picked up on a story and appears likely to publish on it, regardless of the fact that the story was initiated through one alone. Similarly, a respondent organisation may need to disclose to correct what the respondent may regard as inaccurate or misleading information disseminated by media outlets other than the outlet to which a complainant first spoke. A complainant who knowingly takes his or her complaint to 'the court of public opinion' reasonably expects that a respondent organisation will mount its defence in that same forum*.

The individual's expressed expectations

2.47 An individual's desire to control the way in which an organisation uses or discloses their personal information must be balanced against other competing factors. For example, an organisation may be required to disclose an individual's personal information under other legislation (see IPP 2.1(f)). Alternatively, it may not be practicable for an organisation to carry out a particular function such as investigating a complaint, without the disclosure of an individual's personal information. When considering whether a particular use or disclosure is reasonably expected, the actual individual's expressed expectations will be relevant (but not determinative). See the discussion on sensitive and

[13] *Complainant H v Local Council* [2004] VPrivCmr 2 (26 February 2004).

delicate information in the Key Concepts chapter for more information.

Reasonable expectation case studies

2.48 The following case studies provide examples of how VCAT and former Privacy Commissioners have decided whether a use or disclosure of personal information for a secondary purpose is reasonably expected.

Case Study 2C: Disclosure by Council to Complainant's bank during debt recovery proceedings reasonably expected[14]

The Complainant (A), was involved in a dispute with a Local Council (Respondent) concerning an outstanding debt. A provided an employee of the Respondent with information about payments he claimed he had made to pay the amount owing. The employee contacted A's bank to confirm that the payment details were correct. The employee subsequently recorded details of the conversation in a letter to A.

Unable to resolve the dispute, the council commenced recovery proceedings in the Magistrates Court. At a pre-hearing conference the council employee disclosed to the Court details of the conversation between himself and the bank about the disputed debt.

A complained that the employee had unlawfully collected personal information about him by contacting his bank to verify the information given by A and had unlawfully disclosed the information collected to the Court.

In his decision not to entertain the complaint, the Privacy Commissioner noted that IPP 2.1(a) permits an organisation to disclose personal information for a secondary purpose related to the primary purpose where a person might reasonably expect the disclosure to be made. It is an objective test; it is the reasonable expectations of an ordinary person, not expert in the workings of government.

The disclosure of the personal information about A to an officer of a court in pursuit of the debt, at a pre-hearing conference, was related to the primary purpose of collection and could reasonably be expected.

Case Study 2D: Disclosure of personal information to assess whether a student was committing plagiarism reasonably expected[15]

The Complainant was a student of a university (**the University**). Her course coordinator suspected her of plagiarism and sent an email (**the email**) containing allegations about the

[14] *Complainant A v Local Council* [2003] VPrivCmr 1 (17 March 2003).

[15] *Kudleck v Victoria University* (Human Rights) [2013] VCAT 1971 (7 November 2013).

Complainant to the acting heads of school and student progress coordinator.

VCAT held the disclosure of the Complainant's personal information in the email was for the primary purpose of collection. The Tribunal also considered whether the disclosure would have been for a secondary related purpose that was reasonably expected. VCAT found the disclosure was related to the primary purpose of collection and the Complainant would reasonably expect the University would disclose suspicions she had not submitted her own work.

VCAT set out a number of reasons: the course coordinator was required to report such suspicions under the University's academic honesty policy, and the course coordinator was responsible for managing the Complainant's progress under the University's assessment policy, including managing any issues arising from the possibility that she was submitting work that was not her own. The course coordinator did not disclose to mere 'colleagues', but to staff members with responsibilities in relation to a student's progress under the University's assessment policy. It was reasonable to expect a course coordinator to inform the acting heads of school and student progress coordinator about such serious matters prior to a formal meeting and investigation.

Case Study 2E: Use and disclosure of personal information to update records reasonably expected[16]

The Complainant was first registered as a teacher by the Victorian Institute of Teaching (**VIT**) in 2003. One of VIT's powers under the *Education and Training Reform Act 2006* (**the Education Act**) is to maintain a register of teachers. In early 2009 VIT's hearing panel found the Complainant had engaged in serious misconduct and determined to cancel his registration. In late 2009, on appeal, VCAT confirmed the finding of serious misconduct but set aside the panel's decision about cancellation and instead suspended the Complainant's registration until 2011. VCAT imposed conditions on the Complainant's registration, which he had met when he was re-registered as a teacher in 2011.

In the period between his suspension in 2009 and re-registration in 2011, the Complainant changed his name twice.

Following the second name change, VIT updated an existing entry about the Complainant on its website. That entry summarised the conduct dealt with in the 2009 hearings and decisions. The update was to change the heading of the entry from the Complainant's original name to that name together with his name as at July 2011.

The Complainant alleged VIT breached his privacy when it collected information about his changes of name and when it updated the 2009 web page.

VCAT found VIT's use of the Complainant's personal information (updating the existing entry about his conduct to include his new name) was for the primary purpose of collection

[16] *Taylor v Victorian Institute of Teaching* (Human Rights) [2013] VCAT 1290 (3 May 2013).

(to undertake its statutory functions under the Education Act). VCAT also held that, if the disclosure was not for the primary purpose, it would be for a reasonably expected secondary related purpose:

A permissible secondary purpose of collecting the information was to update records which hold the complainant's former name. A reasonable person ought to expect that, where he or she changes his or her name and provides it to an organisation such as the respondent, that new name will be used to refer to him or her. Here, the reasonableness of that expectation is supported by the complainant's prior knowledge of the content of the 2009 web page … A reasonable person who has knowledge of the 2009 web page ought to expect that he will be referred to by his current name on such a page and that may be done in a way which identifies him with the existing records of his past conduct.[17]

Case Study 2F: Disclosure of personal information to third party in complaint handling matter not reasonably expected

The Complainant lived near a property owned by the Organisation. The Organisation had decided to hire the premises out as a venue. The Complainant had previously objected to this use of the premises due to the noise. The Complainant complained to the Organisation about its further hiring out of the venue. In response, the Organisation referred his complaint to the event organisers (who were organising a 'one off' event). The event organisers attempted to contact the Complainant at the Complainant's property to apologise for the noise.

The Complainant was distressed by the disclosure of their personal information (contact details and complaint information) by the Organisation to the event organisers. Such a disclosure in these circumstances would not be reasonably expected because the Complainant had contacted the Organisation to complain, not about the individual event, but about the Organisation's decision to allow the premises to be used as a private space for various events. The Complainant had expressed no interest in engaging with the event organisers. Given the event was a 'one off', any contact between the Complainant and the event organisers could not have resulted in a negotiation about future use of the premises.

Case Study 2G: Disclosure of contact information to third party in complaint handling matter not reasonably expected

The Complainant's backyard was accidentally flooded by a contractor of the Organisation. The Organisation apologised but the Complainant remained dissatisfied.

Several days later the Complainant received a series of calls, some out of business hours,

[17] *Taylor v Victorian Institute of Teaching* (Human Rights) [2013] VCAT 1290 [139]-[141].

from a private number. The caller stated they were one of the contractors who had accidentally flooded the Complainant's yard. The Complainant was confused as to why the contractor was repeatedly calling. The Complainant told the contractor they did not know each other and asked how the contractor had obtained the Complainant's phone number. The contractor explained that the Organisation had provided the contractor with the Complainant's phone number and that the contractor wanted to apologise for flooding the yard.

The use and disclosure of the Complainant's contact information (by both the Organisation and its contractor) was not reasonably expected. While the Complainant might have expected the Organisation (or its contractor) to contact the Complainant for certain purposes (such as facilitating any work required on the Complainant's property), they did not expect a stranger to repeatedly contact them outside of business hours.

Case Study 2H: Disclosure of information relating to student's PhD candidature[18]

A PhD student's ongoing candidature was reviewed by a Tertiary Institution review panel. Having received unfavourable comments from the panel, the student asked his Masters thesis supervisor to review a draft PhD thesis. Prior to doing so, the thesis supervisor spoke to the PhD supervisor about whether the Masters thesis supervisor should be reviewing the thesis, and was advised to not review the thesis as the student's candidature had been terminated. The student complained about disclosure of information about his PhD candidature information to the thesis supervisor. The Privacy Commissioner found that the disclosure was reasonably expected:

It is necessary and appropriate that a PhD supervisor be able to give his or her opinion about whether a thesis supervisor should proceed to review a PhD thesis where the candidate has already been requested by a Review Panel to withdraw as a candidate for a PhD. A person would reasonably expect, absent special circumstances, that two academics with a close working relationship, in the same department, who both at varying points in time supervised the same student, might discuss that student's progression from a degree to a doctorate.

Case Study 2I: Disclosure of complaint details to employee complained of reasonably expected[19]

The Complainants had a son at a local kindergarten, operated by a Local Council. The

[18] *Complainant F v Tertiary Institution* [2003] VPrivCmr 6 (1 December 2003).

[19] *Complainant AG v Local Council* [2007] VPrivCmr 2 (8 June 2007).

complainants wanted to complain about fee advice given to them by their son's kindergarten teacher. They were told to make a written complaint, which they did, and were told it would be kept confidential. The President of the kindergarten disclosed the Complainants' letter to the kindergarten teacher, about whom the complaint related.

The former Privacy Commissioner considered the provisions of IPP 2 and stated:

Where a person raises a complaint with an organisation about the actions of a particular individual within that organisation, it is often necessary to seek a response from the individual who is the subject of the complaint in order to afford natural justice. "Natural justice" requires that where an allegation is made about an individual, and as a result it is proposed that action be taken against the person being complained about, it is only fair that that person be given a right of response in order for the complaint to be properly and fairly investigated.

In light of the particular circumstances of this complaint and despite the parties' conflicting version of events, the allegations against the teacher could not have been adequately addressed unless the teacher was given an opportunity to respond. Therefore, showing the complaint to the teacher was arguably part of the primary purpose of collection, and in any event a related secondary purpose. A reasonable person in the complainants' position should reasonably expect that in the interests of natural justice, where s/he has complained about a specific conversation held with a certain individual, that this individual would have to be consulted about the issue in order to ascertain whether or not there was any basis to the complaint.

Limiting disclosure to what is sufficient

2.49 When disclosing personal information under IPP 2.1(a), organisations should only disclose the amount of information sufficient to satisfy the related secondary purpose (see the following two Case Studies 2J and 2K). Excessive disclosure is not reasonably expected.

Case Study 2J: Avoiding excessive disclosure when handling complaints[20]

The Complainant complained an employee (AC) had misused his position in the Organisation to obtain information about her, and other people, for a personal purpose. Following internal investigation and disciplinary proceedings, the Organisation informed the Complainant of the outcome of its investigation into AC as well as its findings about the wider allegations that other individuals' privacy had been breached.

The Privacy Commissioner found it was reasonably expected that the Organisation would provide sufficient information to the Complainant to show that the investigation of her complaint and outcome were fair. This ensures organisations that deal properly with complaints are seen to do so. However, the Privacy Commissioner considered the disclosure of the results of the wider investigation appeared to involve more information

[20] *Complainant AC v Public Sector Body* [2006] VPrivCmr 4 (28 April 2006).

than was sufficient to deal properly with the Complainant's complaint.

The Organisation acknowledged to AC that its disclosure was excessive and undertook to review its policies concerning the release of information to people who complain about its staff.

Case Study 2K: Avoiding excessive disclosure when handling complaints[21]

The Complainant was an employee of the respondent Organisation and made a bullying claim against co-workers. The complaint documentation consisted of a letter outlining the outcomes the employee sought, and a chronological list of all of the bullying incidents alleged to have occurred. The Complainant met with a staff member of the Organisation who explained the complaint process and advised that a full copy of the complainant documentation would be provided to each of the alleged bullies. The Complainant agreed to this believing there was no other choice. She later attempted to withdraw her consent as she was anxious about the information contained in the complaint documents. The Organisation advised the documents had already been forwarded to the alleged bullies.

In its response, the Organisation argued that, even if it had received the Complainant's withdrawal of consent prior to distribution, disclosing the complaint documentation - in full - was a necessary part of the investigation process. Further, the Organisation argued it was 'not reasonably possible' to edit the complaint documentation before distribution.

The Privacy Commissioner considered the disclosure of the Complainant's information in full to all of the alleged bullies was far more than what they needed to respond to the complaint about their own alleged behaviour. Disclosure of information should have been kept to the minimum necessary to investigate the matter and did not require the wholesale disclosure that had occurred. Similarly, the Privacy Commissioner considered it was possible to edit the documents to protect the Complainant's privacy. The Privacy Commissioner considered that an investigation process requires an organisation to collate the information provided in a complaint and determine what reasonably needs to be disclosed to each staff member.

IPP 2.1(b): Consent

2.50 Consent is one of the exceptions to the rule that personal information can be used and disclosed only for the purpose it was collected for. Organisations can seek consent from an individual to use or disclose information for unrelated or incompatible purposes with the primary purpose of collection, that is, purposes that fall outside the scope of IPP 2.1(a).

2.51 If an individual provides valid consent, the organisation may use or disclose the personal information in a way that is consistent with the consent. Please refer to the Key Concepts chapter for information regarding 'Consent'. Case Study 2L demonstrates the importance of ensuring consent is valid.

[21] *Complainant AU v Public Sector Agency* [2011] VPrivCmr 3 (28 September 2011).

Case Study 2L: 'CP' and Department of Defence[22]

The complainant had lodged a worker's compensation claim with Comcare. Comcare required the claim be assessed by an independent third-party medical practitioner. Although the complainant had previously consented to such disclosures, their consent could be withdrawn at any time.

The complainant had expressly refused permission for their case officer or any other Defence personnel to contact their medical practitioners. Defence personnel disclosed the third-party medical practitioner's report to the complainant's GP despite this.

The complainant alleged that the Department of Defence had interfered with their privacy by disclosing sensitive personal information about them to a third party, their GP, without consent and after they had expressly refused to grant consent of the report to their GP. The complaint was upheld.

Sharing information where consent has not been provided

2.52 In cases where an individual has not provided consent to use or disclose their personal information, this will not necessarily mean an organisation will be unable to use or disclose the information. Other exceptions under IPP 2, such as disclosure authorised or required by or under law (IPP 2.1(f)), may allow a disclosure to proceed irrespective of whether the individual has consented.

Distinguishing consent from notice

2.53 Organisations must distinguish consent from notice (provided by a collection notice, under IPP 1.3). Often individuals have no real choice in a use or disclosure when transacting with government. In such circumstances, when the individual signs a form it is usually regarded as an acknowledgement that he or she has received notice. It is not 'consent' in the proper sense of the word. The differences between notice and consent are discussed further under Consent in the Key Concepts chapter.

Opting-in is the preferred approach

2.54 If an organisation is seeking to rely on consent as the authority to use or disclose information, it should be opt-in consent. The opt-in method demonstrates more reliably that the individual has actively consented compared to the opt-out method. For more information, the opt-in and the opt-out consent models are discussed under 'Opt In versus Opt Out' in the Key Concepts chapter.

IPP 2.1(c): Necessary for research or statistics in the public interest

2.55 IPP 2.1(c) allows organisations to use and disclose personal information necessary for research or the compilation or analysis of statistics when three requirements are met:

- The research is in the public interest;

[22] *'CP' and Department of Defence* [2014] AICmr 88 (2 September 2014).

- The information is not for publication in a form that identifies any particular individual; and
- It is impracticable for the organisation to seek the individual's consent before the use or disclosure.

2.56 In the case of disclosure, the organisation must also reasonably believe the recipient of the information will not disclose the information.

Necessary for research or compilation or analysis of statistics

2.57 For organisations to use and disclose personal information under IPP 2.1(c), the use and disclosure must be necessary for the research or statistical work. Use or disclosure will not be necessary when the same research objectives can be achieved with alternative sources of data or data that has been de-identified or is anonymous. When developing research projects, organisations should consider if the same objectives could be achieved without using personal information.

2.58 Before organisations rely on IPP 2.1(c) to use or disclose personal information (or for any project or initiative that poses a risk to the privacy of individuals), they should consider completing a privacy impact assessment (**PIA**). PIAs are a tool to assist organisations identify potential privacy risks and ways to mitigate them before personal information is handled.[23]

Key terminology

2.59 'Research' is not defined in IPP 2.1(c). As such, the word should be given its ordinary meaning. Research is a systematic investigation and study which seeks to establish new facts and reach new conclusions. It is more than a reorganisation of data or restatement of facts. Research begins with a clearly defined goal and the information gathered aims to help reach that goal.

2.60 'Statistics' are numerical data, especially when large quantities are involved. Compilation is the collection of numerical data and analysis involves an undertaking of detailed examination of the data and inferring conclusions about the information or the set or a subset of data subjects.

Research 'in the public interest'

2.61 Organisations can only rely on IPP 2.1(c) to use or disclose personal information for research or statistical work without individuals' consent when the work is in the public interest.

2.62 To determine whether a proposal for research or statistical work is 'in the public interest', organisations should be explicit in their definition of the public interest and how the research promotes this public interest. Organisations should consider the following questions:

- Is the organisation considering the public interest as broader than its own needs?
- What is the public importance of the research?
- How will the wider community benefit from the research or statistical work? Will the community benefit, for example, by:
  - gaining in greater knowledge, insight or understanding within fields such as science and humanities;
  - the improvement of social welfare, public safety or individual well-being, or the minimisation of serious harm, or;
  - the enhancement of the delivery of government services or the targeting of government funded welfare or educational services?

[23] For more information, see OVIC, 'Privacy impact assessments'.

- Are there any countervailing interests to consider to balance the public interest in privacy and the public interest in the conduct of the research?
  - Is there a cost to the community of not undertaking the research or statistical work?
  - Are participants at risk of any harm (for example, physical, emotional, social, economic or legal harm)? If so, what is the seriousness and likelihood of this harm?

2.63 The National Health Medical Research Committee has published Guidelines approved under s 95A of the Commonwealth *Privacy Act 1988*. Although not directly applicable to the PDP Act, these Guidelines provide additional questions and considerations which may help an organisation determine whether their research is in the public interest.

2.64 A research ethics committee may also help an organisation assess whether the research involving personal information is in the public interest. Some organisations, such as universities, may be required due to their funding or other arrangements to consider the National Statement on Ethical Conduct in Human Research.[24] Some Departments also have research committees, for example, the Department of Justice and Community Safety requires ethics approval from this research committee where a researcher wishes to use departmental data and the risk or discomfort to participants is greater than low or the research involves vulnerable or disadvantaged individuals.

Not for publication in a form that identifies any particular individual

2.65 To use and disclose personal information under IPP 2.1(c), organisations must ensure the research or statistical work is not for publication in a form that identifies any particular individual. This means organisations should de-identify personal information prior to publication to ensure published material does not contain personal information. Organisations should not consider de-identification as a final end state. Instead, organisations should always consider the possibility of re-identification, especially when data is drawn from small communities or data sets. For more information, see 'De-identified information' in Key Concepts.

'Impracticable' to seek consent

2.66 Impracticability means more than mere inconvenience or some cost or effort for a public sector organisation. The impracticability of seeking consent should not be confused with the undesirability of seeking consent. IPP 2.1(c) does not permit consent to be waived where consent can be readily sought but organisations would prefer not to do so in order to achieve greater participation. Impracticability must be assessed in context.

2.67 The quantity, age or accessibility of records may make it impracticable to obtain.[25] According to the NHMRC's National Statement on Ethical Conduct in Human Research, it is usually impractical to obtain consent from individuals for secondary use of information collected during the delivery of a service by a government department because the collection of information may involve large numbers of people or whole populations. For example, it may be impracticable to seek consent where the organisation is unable to locate the individual, despite making reasonable efforts.

Reasonable belief the recipient will not disclose information

2.68 In the case of disclosure only, there is an additional requirement: organisations must reasonably believe the recipient of the information will not disclose that information. To be able to demonstrate a reasonable belief under IPP 2.1(c)(ii), organisations should ensure they keep records of the

[24] National Statement on Ethical Conduct in Human Research (2007, updated 2018).

[25] National Statement on Ethical Conduct in Human Research (2007, updated 2018) Chapter 2.3.

following considerations (among others):

- Does the organisation reasonably believe that the recipient of the personal information will not further disclose the information?
- Have undertakings or agreements of confidentiality been sought?

2.69 Where the disclosure is outside of Victoria, have appropriate privacy protection measures been attended to in accordance with obligations under IPP 9 (Transborder Data Flows)? Case Study 2M illustrates the points organisations need to consider when seeking to rely on IPP 2.1(c).

Case Study 2M: Personal information sought for research in the public interest

A research institution sought information from a local Council to conduct research relating to the State farming industry and livestock. The Council was asked to disclose information relating to historical land ownership and farming permits under local laws which contained personal information about past and present residents.

The institution's ethics committee had considered the proposed research and decided that it was in the public interest.

The institution provided the Council with written confirmation it understood and agreed the information supplied was confidential, only for the purpose of the specified research and not to be published in any way that would allow identification of particular individuals.

The Council made records of its evaluation of the necessity of the information for the research. The information was not publicly available or easily ascertainable. It was impracticable to obtain consent because contact details in the historical land ownership records were out of date, in spite of reasonable efforts on the part of the Council and research institution to find them.

The disclosure of the information by the Council was subject to a series of requirements:

- The information was to be used by the research institution only for the research in question.
- The information could not be retained by the research institution after the current research was completed.
- The information could not be supplied to any third parties.
- The published results of the investigation would contain no personal information.

The undertakings by the institution and the Council's additional requirements for disclosure were sufficient for the Council to demonstrate it had met its obligations under IPP 2.1(c).

Other grounds which may permit research or compilation or analysis of statistics

2.70 The PDP Act facilitates the conduct of research in a number of ways which are not limited to the use and disclosure ground in IPP 2.1(c). Organisations should consider these alternatives before

disclosing personal information to researchers or conducting research themselves. These include:

- using de-identified data;
- where the research is related to the organisation's functions or activities and is reasonably expected, organisations can rely on IPP 2.1(a) to make first contact with prospective participants on the behalf of the researcher. For example, a school may initiate contact with students and their families about education-related research. Here, the public interest in privacy and the public interest in research are balanced, by the organisation maintaining control over the information it holds and only disclosing identifiable details after consent has been obtained by those individuals wishing to participate in the research;
- relying on the valid consent of an individual for the future use or disclosure for research or statistical work obtained when the personal information is collected (under IPP 2.1(b));
- where the disclosure is necessary to lessen or prevent a serious threat to public health, safety or welfare under IPP 2.1(d); and
- where the disclosure is required and authorised by law and IPP 2.1(f) applies. For example, s 34 of the *Electoral Act 2002* (Vic) expressly authorises disclosure of enrolment information in the public interest after consultation with the Information Commissioner.

Notification after use or disclosure and withdrawal

2.71 Where it is impracticable to seek consent before the research subject's personal information is used, organisations may still notify the person after the use or disclosure. Notification is distinct from consent, but it does provide individuals with an opportunity to withdraw from further participation in the research study. This is consistent with ethical research standards supporting revocation of consent.

IPP 2.1(d): Necessary to lessen or prevent serious threats to health or safety

2.72 IPP 2.1(d) allows use or disclosure to occur where the organisation reasonably believes it is necessary to lessen or prevent:

- a serious threat to an individual's life, health, safety or welfare; or
- a serious threat to public health, public safety or public welfare.

2.73 This section requires two things of organisations which seek to rely on this exception for the use and disclosure of personal information. An organisation must form a reasonable belief there is a serious threat and it must believe the use or disclosure is necessary to lessen or prevent the threat. What an organisation believes on reasonable grounds 'is very much a matter to be decided on the evidence of each case'.[26] To decide whether there are reasonable grounds for belief, organisations should consider the source and reliability of the information that indicates the threat and the seriousness of the indicated threat.[27]

2.74 Legislative reforms in 2017 removed the word 'imminent' from IPP 2.1(d)(i). These reforms are discussed below under the heading 'Removal of the word 'imminent''.

[26] *TYGJ and Information Commissioner* [2017] AATA 1560 [289] (which considered the equivalent provision under Commonwealth privacy law).

[27] *TYGJ and Information Commissioner* [2017] AATA 1560 [37].

'Reasonably believes'

2.75 For IPP 2.1(d) to permit use or disclosure for a secondary purpose, the organisation must *reasonably believe* that the disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare. This means the belief is not a wholly subjective matter. There must be circumstances in which it is reasonable for the organisation to form the belief. Whether a belief is reasonable is to be determined at the time of disclosure. Later circumstances cannot be relied on to make a belief reasonable.[28]

Case Study 2N: Requirement for a reasonable belief that disclosure is necessary

In *McMahon v RMIT University*,[29] a university student complained that a professor had breached IPP 2 by disclosing a variety of information about him for the purpose of seeking and subsequently defending an intervention order.

VCAT found the disclosures and use were permitted under IPP 2.1(d) because the professor had a reasonable belief that the disclosures and use would lessen a serious threat to his safety. The circumstances which made the professor's belief in necessity of disclosure *reasonable* were:

- an aggressive email to the professor's staff;
- a Facebook page seeking information about the professor; and
- a disturbing YouTube clip that implied serious violence and was extremely abusive.

Although the second two points did not have the student's name attached, VCAT considered that it was reasonable for the professor to believe the student was the author of, or connected with, the abusive material on the internet due to the coincidence in time of discipline events affecting the Complainant.

VCAT also accepted it was reasonable to believe the disclosures and use would lessen the threat and that this belief continued at the time of disclosure and use.

'Necessary'

2.76 It is not enough for an organisation to form a reasonable belief there is a serious threat. IPP 2.1(d) also requires the organisation believe it is necessary to disclose information to lessen or prevent the threat. 'Necessary' in this context has been interpreted as 'that which is … needed; essential; indispensable; that must be done'.[30]

2.77 In determining whether a use or disclosure might be regarded as necessary, organisations should

[28] *McMahon v RMIT University* (Health and Privacy) [2012] VCAT 1423, [82].
[29] *McMahon v RMIT University* (Health and Privacy) [2012] VCAT 1423.
[30] *TYGJ and Information Commissioner* [2017] AATA 1560 [289].

consider:

- Is the use or disclosure motivated by an intention to lessen or prevent the threatened harm?
- Is the information being used or disclosed relevant to managing that threat?
- Where information is disclosed, is the recipient in a position to act on the information to lessen or prevent the harm from eventuating?

2.78 IPP 2.1(d) does not specify who can use the information or to whom it may be disclosed. In most cases, the recipient would need to be an appropriate agency in a position to lessen or prevent the particular threat. For example, and depending on the circumstances, appropriate recipients would be the police, emergency services or health authorities.

'Serious'

2.79 Whether or not a threat can be considered 'serious' for the purposes of the PDP Act should take into account what a reasonable person would regard as 'serious'. In making an assessment as to whether a threat is 'serious', organisations should consider the following factors:

- **Severity** - How significant are the consequences of the threat?
- **Likelihood** - What is the chance of the threat actually happening? What is the relative likelihood that harm will occur?

2.80 Serious has been used, in the context of IPP 2.1(d), in the sense of being 'important' or 'grave'.[31]

2.81 There are a range of circumstances that may impact upon the seriousness of a threat. It may not be clear in all situations whether a threat is likely to ever happen or how severe the consequences might be for an affected individual. In these cases, organisations may wish to look at secondary factors applicable to the particular situation in making an assessment as to the severity and likelihood of the threat. These factors may include, but are not limited to:

- **Timing** - How soon is the threat likely to occur? Is the threat ongoing?
- **Nature of the harm** - What is the level of perceived harm to the individual? What type of harm is likely to result (for example, physical, mental, financial)?
- **Vulnerability** - Considering the circumstances, how vulnerable might the affected individual be to the threat (for example, is the victim a child?)

2.82 These secondary factors may not be relevant in every case, but in some situations, may assist in making an assessment as to whether a threat is 'serious'. Seriousness should be determined on a case by case basis, as the circumstances surrounding a threat will differ.

Removal of the word 'imminent'

2.83 Legislative reforms in 2017 removed the word 'imminent' from IPP 2.1(d)(i). Previously, organisations could only rely on this exception to disclose information in response to a threat that was imminent. While the legislative change in Victoria came about in the context of family violence prevention, the removal of 'imminent' has a broader application. The removal of 'imminent' means organisations need only establish a threat is serious, and that disclosure is necessary to lessen or prevent that threat is necessary, before relying on IPP 2.1(d)(i) to use and disclose personal information.[32] Case Study 2O illustrates the effect of this change.

[31] *McMahon v RMIT University* (Health and Privacy) [2012] VCAT 1423 [84].
[32] See also: OVIC, 'Removal of 'imminent' from the IPPs and HPPs' (Fact sheet).

Case Study 2O: The effect of the removal of 'imminent'

A client of a health service is behaving aggressively and has made threats towards staff. The health service manager is considering whether to exclude the person from attending the health service in the future. The manager is aware the client also receives services from another organisation and is considering contacting the other organisation to seek information about the client that may justify excluding him from the health service. Previously, the manager may not have been able to collect the client's health information from the other organisation unless the threat was expected to be carried out in the immediate future. Now, the manager can collect the information if the threat is serious and staff are at risk, even if the timing of a possible future incident is unknown.

Public sector employees acting on information obtained in their private capacity

2.84 Public sector employees may come across information in their private capacity that leads them to believe or suspect someone poses a serious risk to an individual's or the public's health, safety or welfare. Public sector employees may be tempted to use their privileged access to official information (such as criminal records or child protection files) to confirm their suspicions and decide to use or disclose the information in their private capacity. This situation may create difficulties for an organisation which has a function to protect the community from threats of harm but also has obligations to prevent sensitive information it holds from being used or disclose in an unauthorised manner. Organisations should balance all relevant interests including the protection of a well-meaning staff member from later accusations of wrongful use of databases.

2.85 Factors relevant to determining whether the official's use or disclosure is necessary to lessen or prevent a serious harm might include:

- the reliability of the information obtained in the official's private capacity;
- the seriousness of the potential harms;
- the degree of vulnerability of the potential victims (including whether they are in a position to recognise the threat themselves); and
- the involvement of an appropriate authorised person.

Anticipating the need to provide information during an emergency

2.86 Where there is a serious threat to public health or safety, for example, an infectious disease or large-scale evacuation, significant amounts of personal information could be required. Additionally, threats to health, safety or welfare in this context will generally require a fast and appropriate response from the organisation. Steps to ensure limited disclosure consistent with the circumstances should be developed by organisations prior to an emergency situation.

2.87 Organisations are advised to have and communicate a policy that covers the use and disclosure of personal information in the event of an emergency, so organisations can quickly and confidently handle a request for personal information.

Using or disclosing during emergency relief efforts

2.88 IPP 2.1(d) may also be relevant to information uses and disclosures after a disaster or accident has

occurred to assist emergency services, for example, in locating victims and reuniting them with their family, ensuring victims receive medical attention and ensuring they have the opportunity to take advantage of various other forms of support (such as financial assistance and counselling). Such disclosures are likely to be permitted under IPP 2.1(d) as lessening or preventing serious harm to public welfare.

2.89 'Public welfare' in this context includes offering assistance to victims to assist the community more generally to overcome the effects of disasters and other trauma. It is legitimate for authorities to try to reach victims to offer support, however, authorities must also be aware not everyone responds to offers of support in the same way. Disaster victims can always decline offers of support made by or on behalf of government agencies and their wishes for no further contact should be respected.

IPP 2.1(e): Investigating suspected unlawful activity

2.90 Where an organisation has reason to suspect that unlawful activity has been, is being, or may be, engaged in, IPP 2.1(e) allows personal information to be used or disclosed:

- as a necessary part of the organisation's investigation of the matter; or
- in reporting the organisation's concerns to relevant persons or authorities.

2.91 This ground for use and disclosure should not be used lightly as it has serious privacy implications. It should not be used for speculative monitoring, surveillance or intelligence gathering. There must be a reasonable basis for suspecting unlawful activity. However, it is not necessary that unlawful activity has in fact occurred; even if the organisation's suspicion eventually turns out to be unwarranted, disclosure will still have been authorised if the circumstances described in IPP 2.1(e) are met.[33]

Unlawful activity

2.92 The activity being investigated must be unlawful, not simply unethical or objectionable. Suspected breaches of the criminal law would fall within the meaning of 'unlawful activity'. However, 'unlawful' should not be interpreted as limited to criminal activity. It can also include activity contrary to civil law and rules.[34]

2.93 Misconduct by public sector employees may also be considered unlawful if it contravenes a statutory prohibition, such as a secrecy obligation. For example, IPP 2.1(e) may be relied upon to enable a department to investigate and report misconduct concerns to human resources in relation to workplace discrimination or harassment, because there are statutory prohibitions against this behaviour.

2.94 Misconduct may also be considered unlawful if it involves conduct that may result in the imposition of a penalty or other sanction, such as the types of misconduct set out in the *Public Administration Act 2004* (Vic).[35] See Case Study 2P for more information.

[33] *Zegaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018) [96].

[34] *McLean v Racing Victoria Ltd* [2019] VSC 690 [63]-[66].

[35] Section 22 of the *Public Administration Act 2004* (Vic) defines 'misconduct,' for which penalties (including a salary reduction, demotion, suspension or dismissal) may be imposed, to include: (a) a contravention of a provision of the Public Administration Act, the regulations or a binding code of conduct; (b) improper conduct in an official capacity; (c) a contravention, without reasonable excuse, of a lawful direction given to the employee as an employee by a person authorised (whether under this Act or otherwise) to give the direction; (d) an employee making improper use of his or her position for personal gain; (e) an employee making improper use of information acquired by him or her

Case Study 2P: Disclosure during investigation of serious misconduct allegations[36]

The Complainant, an employee of the Organisation, was the subject of serious misconduct allegations. The Organisation disclosed personal information (including his bank account and holiday and sick leave details) about the employee to an external investigator for the purposes of enquiring into the alleged misconduct. The Organisation also appointed a review panel to independently assess the investigator's report.

The Organisation argued that IPP 2.1(e) applied to its investigation of allegations of misconduct by the complainant because that conduct raised issues of breaches of the Code of Conduct provisions, given legislative force under the *Public Sector Employment and Management Act 1998* (Vic) [which has been replaced by the *Public Administration Act 2004* (Vic)], and s 95 of the *Constitution Act 1975* (Vic).

The Privacy Commissioner considered that IPP 2.1(e) permits the use and disclosure of personal information at any stage of an investigation into serious misconduct for the purposes of determining whether the suspected activity is taking place. While noting that it is likely for disclosures during an investigation to involve a mix of personal information that may or may not be relevant to the investigation, in this case, the information was necessary to the investigation. Accordingly, the Privacy Commissioner declined the complaint on the basis that there had not been an interference with privacy.

Nevertheless, to avoid future confusion, the Department decided to amend its serious misconduct policy to expressly state that an employee's personnel file could be disclosed to an internal or external investigator for the purpose of understanding an allegation of serious misconduct.

2.95 In *Kudleck v Victoria University* (Human Rights) [2013] VCAT 1971 (see Case Study 2D), VCAT found that 'unlawful activity' does not include activities that may constitute disciplinary offences created through regulations made under Part 5 of the *Victoria University Act 2010* (Vic). This was because a regulation made under that Act is not a statutory rule under the *Subordinate Legislation Act 1994* (Vic) nor a subordinate instrument for the purposes of s 32 of the *Interpretation of Legislation Act 1984* (Vic). Therefore, VCAT found IPP 2.1(e) did not authorise the use or disclosure by Victoria University.

Investigation by the organisation

2.96 When an organisation proposes to use or disclose personal information to investigate suspected unlawful activity, the organisation should be aware that:

- any suspicion of wrongdoing should be based on reasonable grounds, not unsubstantiated

by virtue of his or her position to gain personally or for anyone else financial or other benefits or to cause detriment to the public service or the public sector.

[36] *Complainant I v Department* [2004] VPrivCmr 4.

gossip or rumour;

- the use or disclosure must be considered necessary after due consideration of alternatives; and
- the use or disclosure should be as confined as possible throughout the organisation's investigation, both in terms of the number of individuals whose information is involved and the number of people who are given access to the information.

2.97 Personal information may be used or disclosed at any point during an investigation into unlawful activity or serious misconduct. See Case Study 2P above, concerning *Complainant I v Department* [2004] VPrivCmr 4.

2.98 Any organisation to which the PDP Act applies may investigate suspected unlawful activity or refer its concerns to a relevant person or authority (disclosing the information).[37] Investigations or reporting of concerns under IPP 2.1(e) are not limited to criminal investigations of law enforcement agencies. For example, in *McLean v Racing Victoria Ltd* [2019] VSC 690, Victoria Police was permitted to disclose personal information to Racing Victoria because Victoria Police had reason to suspect unlawful activity had been engaged in, and the disclosure to Racing Victoria was 'reporting its concerns to the relevant persons or authorities', as under IPP 2.1(e).

Disclosure to relevant persons and authorities

2.99 When an organisation decides to report suspected unlawful activity, such use or disclosure should be limited to the persons or authorities with a need to know the information because they have relevant duties to perform in the circumstances. Examples include law enforcement organisations, an organisation responsible for the protection of public revenue, such as the State Revenue Office, or regulatory authorities such as the Food Safety Council.

Case Study 2Q: Disclosure by law enforcement authority to a third party

In *Zegaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018), the Complainant complained that the Respondent interfered with his privacy by disclosing his personal information to third parties.

The Complainant complained the Respondent disclosed to the Australian Taxation Office (**ATO**) that he:

- was the subject of an investigation. This alleged inappropriate disclosure occurred when the Respondent sent a notice to the ATO requesting information about the Complainant in 2011; and
- had been identified as being involved in the cultivation, distribution and sale of cannabis. This alleged inappropriate disclosure occurred when the Respondent responded to a request for information about the Complainant from the ATO in 2012.

VCAT held the ATO disclosure was consistent with the Respondent's primary purpose of collection of personal information under IPP 2.1. It noted that even if the disclosure was not consistent with the Respondent's primary purpose, the disclosure would fall under the investigating unlawful activity exception [IPP 2.1(e)] or the required or authorised by law

[37] *McLean v Racing Victoria Ltd* [2019] VSC 690 [65].

exception [IPP 2.1(f)].

Notice of disclosures under IPP 2.1(e)

2.100 Any organisation wishing to use or disclose an individual's personal information under IPP 2.1 should consider if it has taken reasonable steps to provide the individual with notice as required under IPP 1.3. Disclosures under IPP 2.1(e) are no exception. Relevant factors for consideration include:

- the source of the information – consider whether the information has been obtained from a suspect, a victim or witness; and
- the nature of the unlawful activity – whilst the activity must be 'unlawful' (rather than simply objectionable or unethical, as discussed above), this will capture a broad range misconduct, some more serious or 'sensitive' than others.

2.101 The reasonableness of providing notice of a disclosure under IPP 2.1(e) needs to be determined on a case by case basis. It would be unreasonable to provide notice of an IPP 2.1(e) to a suspect. It may be reasonable to provide notice of an IPP 2.1(e) to a victim of an unlawful activity that is particularly 'sensitive', for example, sexual assault.

IPP 2.1(f): Required or authorised by law

2.102 IPP 2.1(f) allows personal information to be used or disclosed for a purpose other than the primary purpose if such use or disclosure is required or authorised by or under law.

Required by law

2.103 'Required by law' means there is a legal obligation to use or disclose personal information in a particular way.[38] Words such as 'must' or 'shall' will indicate a requirement and may be accompanied by the presence of a sanction for non-compliance. 'Requires' includes demands or necessities and extends to warrants, court orders and statutory provisions.[39] One type of statutory provision that is often relevant to IPP 2.1(f) is the power to demand the production of documents or information.

Case study 2R: 'OJ' and the Department of Home Affairs[40]

The Complainant made a complaint relating to disclosure of their personal information by the Department of Home Affairs (**DHA**), to the Department of Human Services Victoria (**DHSV**) and the Minister for Home Affairs, in responding to a request for information by the television show 'A Current Affair' (**ACA**).

DHSV complaint

The Complainant's personal information, including their immigration status, was disclosed

[38] *Department of Premier and Cabinet v Hulls* [1999] VSCA 117, [31] (Phillips JA).

[39] *Department of Premier and Cabinet v Hulls* [1999] VSCA 117, [31] (Phillips JA); *Zegaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018) [98].

[40] *'OJ' and the Department of Home Affairs* [2018] AICmr 35 (19 March 2018).

to DHSV by DHA in response to a subpoena issued by the Federal Circuit Court. The disclosure of the Complainant's personal information by the DHA was required by the *Federal Circuit Court of Australia Act 1999* (**FCCA Act**) and the Federal Circuit Court Rules 2001 (**FCC Rules**). These laws make it an offence to not comply with a subpoena. As a result, the Australian Information Commissioner found there was no interference with the Complainant's privacy as the disclosure was required by law.

ACA Complaint

ACA had requested information in writing in relation to the Complainant's circumstances and status of the deportation order against the Complainant (among other things). The ACA's request for information included the Complainant's name, the location of the detention centre that the Complainant was held in and details regarding their immigration visa status.

The request for information and the response prepared by the DHA's Portfolio Media Unit was forwarded to the Minister for Home Affair's media adviser.

The Information Commissioner was required to determine whether the DHA's use of the Complainant's personal information and disclosure to the Minister's office was authorised or required by law.

The Commissioner found it was necessary for the Department to disclose the information in the ACA request to the Minister's Office, under s 57(2) of the *Public Service Act 1999* (**PS Act**). Section 57(2)(b) requires the Secretary of a Department to advise the Minister about departmental matters.

2.104 In *Dodd v Department of Education and Training*,[41] VCAT found the Department's disclosure of two documents to the Victorian Institute of Teaching (**VIT**) fell within IPP 2.1(f). The documents consisted of Mr Dodd's exchange of letters with a teacher about the veracity of her evidence before a disciplinary hearing held by the Department in relation to the conduct of another teacher. VCAT found the disclosure was in accordance with s 27(2) of the *Institute of Teaching Act 2001* (Vic) which requires the Department to provide the VIT with any information the VIT might reasonably require to conduct its enquiry. The Department was acting under a mandatory duty to provide the information.

Authorised by law

2.105 The phrase 'authorised by law' refers to a law which permits the use or disclosure but does not make it compulsory.[42] Words such as 'may' are indicative of this. An authorising power must be reasonably specific; a general power or function for 'anything incidental' would be insufficient.

2.106 Authorisation under law need not be confined to a specific statutory duty under an Act but may extend to other common law duties or authorities for disclosure.

[41] *Dodd v Department of Education and Training* (General) [2005] VCAT 2207.

[42] *Zegaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018) [98].

Case Study 2S: disclosing information to court officers permitted[43]

In a pre-hearing conference, a Local Council disclosed personal information about the person bringing the action against the Council. The person claimed that the disclosure in the pre-hearing conference was an infringement of his privacy. The Local Council asserted that the disclosure was authorised by law under IPP 2.1(f).

The Privacy Commissioner determined that the law permits, and in some cases requires, persons to give information to officers of the court, or evidence to a court about matters relevant to a case. It is the person presiding over the pre-hearing conference or the hearing who decides what is relevant. Accordingly, the Privacy Commissioner considered the disclosure to be a permitted disclosure under IPP 2.1(f).

Administrative release of information under section 16(2) of the FOI Act

2.107 Section 16(2) of the *Freedom of Information Act 1982* (Vic) (**FOI Act**) authorises organisations to make information (including documents that might otherwise be exempt under the FOI Act) available to the public informally, without requiring individuals to lodge a formal written request for access under the FOI Act, where the organisation can properly do so or is required by law to do so. This procedure for publishing or disclosing documents outside of the FOI Act is sometimes referred to as 'administrative release'.[44]

2.108 Section 16(2) of the FOI Act only authorises disclosure where organisations can 'properly do so' or are required by law to do so. It would not be 'proper' to give access under s 16(2) of the FOI Act where this would involve an unreasonable impact on the personal privacy of an individual or breach of some other legal obligation. Organisations should also consider whether it would be proper to release information having regard to:

- any relevant duties of confidentiality or statutory secrecy requirements; and
- existing legal obligations under the PDP Act not to disclose personal information about any person for a purpose other than the primary purpose of collection unless the disclosure is in accordance with IPP 2.1(a)-(h).

Disclosing only to the extent required or authorised

2.109 In some cases, the legislative authority behind the information request or demand may be conditional or limited in some way. For example, the legislation may require an investigation to be formally established before a demand for information can be issued to obtain information to assist in that investigation.

2.110 When disclosing information, it is important to disclose only information that is required by the request. There might be circumstances where information is privileged and therefore may not be disclosed. If required seek additional information from the requestor about the information being sought and the authority or requirement under legislation to collect the information, to ensure that

[43] *Complainant A v Local Council* [2003] VPrivCmr 1.

[44] See, for example, Victorian Ombudsman, *Review of the Freedom of Information Act*, discussion paper, May 2005, available at http://www. ombudsman.vic.gov.au, pages 44-46.

the disclosure includes only what information is required under the request.

Case Study 2T: publication of personal details in tribunal decision not authorised or required by law

In *Le and Secretary, Department of Education, Science and Training* [2006] AATA 208, the Administrative Appeals Tribunal (**AAT**) considered the federal equivalent to IPP 2.1(e) to determine how much information should be included in a published AAT decision. In that case, the applicant's daughter was searching for her family name on the internet when she came across an AAT decision on Austlii. The decision related to her father's application to the AAT to review a Department of Employment, Education and Training decision that he not be paid Austudy at the student homelessness rate. The decision revealed quite explicit details, including addresses of relevant persons and details of the applicant's relationship with his parents.

The AAT considered principles of open justice and its statutory obligations under the *Administrative Appeals Tribunal Act 1975* (Cth) (**AAT Act**) to hear matters in public and to publish its reasons for decisions. The AAT found that its decisions need only publish as much of a person's information as is necessary to disclose adequately the intellectual process that resulted in the particular decision.

In the applicant's case, the AAT had gone beyond what was necessary to fulfil its obligations and may exercise its power under the AAT Act to restrict access to personal information. Accordingly, the AAT made an order to restrict publication of the addresses of the applicant and his parents as not being authorised or required under law.

IPP 2.1(g): Reasonably necessary assistance for law enforcement and protection of public revenue

2.111 IPP 2.1(g) allows an organisation to use or disclose personal information where the organisation reasonably believes the use or disclosure is reasonably necessary for any of five specified purposes undertaken by or on behalf of a law enforcement agency. Under IPP 2.1(g), organisations *may* share information; it is not mandatory. Some organisations prefer to share certain information only in response to subpoena, warrant, court order or equivalent request for information.

2.112 The five specified purposes are:

- the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
- the enforcement of laws relating to the confiscation of the proceeds of crime;
- the protection of the public revenue;
- the prevention, detection, investigation or remedying of seriously improper conduct; or
- the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

2.113 If an organisation uses or discloses personal information to assist law enforcement agencies for any of the above purposes, IPP 2.2 requires the organisation to make a written record of that use or

disclosure. Please refer to the section discussing IPP 2.2 for further information. Refer to IPP 2.2 below for further information.

Law enforcement agency

2.114 IPP 2.1(g) authorises disclosure to law enforcement agencies. 'Law enforcement agency' is defined in s 3 of the PDP Act. The definition specifically includes state and federal police, crime commissions and examiners, the Business Licensing Authority and the Special Investigations Monitor. The definition also includes agencies involved in the prevention and detection of crime, the release of persons from custody, the execution of warrants, the provision of correctional services, the management and seizure of property under confiscation laws and the protection of public revenue. Many Victorian government departments and agencies have some law enforcement functions.

2.115 IPP 2.1(g) also authorises disclosure to persons who carry out any of the five functions (listed above) on behalf of a law enforcement agency. For example, this includes lawyers preparing matters for trial. The Explanatory Memorandum of the PDP Act says IPP 2.1(g) and (h) are intended to give latitude to organisations disclosing personal information to law enforcement agencies.

Reasonably believe disclosure is reasonably necessary

2.116 Organisations are not prevented by the PDP Act from cooperating with law enforcement agencies. IPP 2.1(g) expressly authorises organisations to assist law enforcement agencies by providing information relevant to law enforcement functions. However, IPP 2.1(g) requires organisations to make a judgement about whether the use or disclosure is reasonably necessary in the circumstances. The tests of 'reasonable belief' and 'reasonable necessity' must be satisfied.

2.117 In *Zeqaj v Victoria Police*,[45] VCAT held Victoria Police did not have reasonable belief the disclosure was reasonably necessary because they had not considered whether departure from the IPPs was reasonably necessary. VCAT required evidence of this reasonable belief being formed for IPP 2.1(g) to authorise the use of the personal information.

2.118 Organisations must 'reasonably believe' it is 'reasonably necessary' to disclose the information for one of the specified purposes in IPP 2.1(g)(i)-(v). IPP 2.1(g) requires the organisations to make a judgement in the circumstances as to whether the use or disclosure is necessary.

2.119 The organisations should also take steps to satisfy itself that use and disclosure is reasonably necessary for the specific law enforcement function. However, these steps do not need to be extensive. In determining when it is reasonably necessary to disclose, the Explanatory Memorandum to the PDP Act suggests: [46]

> *Minimal information about the purpose of collection by the law enforcement agency would usually be enough to establish that the disclosure was 'reasonably necessary.'*

2.120 Further information on assessing a request is provided under the heading 'Assessing a request for information for a law enforcement function'.

2.121 In some cases, organisations may determine it is inappropriate to release the information under IPP 2.1(g). This may be because they have not been persuaded the information is necessary for one of the authorised purposes. Or the organisation may determine that, due to the sensitivity or volume of information requested, it would be more appropriate to withhold the information until and unless a

[45] *Zeqaj v Victoria Police* (Human Rights) [2018] VCAT 1733 (20 November 2018).

[46] Explanatory Memorandum, Privacy and Data Protection Bill 2014 (Vic) 35.

warrant or other legal authority is produced.

2.122 Any use or disclosure of personal information under IPP 2.1(g) must be noted by the organisation in writing (see IPP 2.2).

Specified law enforcement purposes

2.123 Although the range of authorised recipients is broad, the authority to disclose under IPP 2.1(g) is limited. Use or disclosure must be tied to one of the five specified purposes, explained in more detail below.

IPP 2.1(g)(i): the prevention, detection, investigation, prosecution or punishment of crime and other breaches of the law criminal offences or breaches of a law imposing a penalty or sanction

2.124 IPP 2.1(g)(i) allows information to be used or disclosed for the purpose of prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction.

2.125 A criminal offence is an act or practice that is prohibited by criminal law at Commonwealth, State or Territory level. 'Penalty' generally refers to a punishment, including a fine or monetary payment. 'Sanction' generally refers to some other legal requirement, order or action used to punish non-compliance with a law. Common sanctions include revocation of a licence, withdrawal of a benefit or disciplinary actions such as suspension or dismissal.

2.126 In *Complainant AB v Victoria Police*,[47] fingerprints from applicants for firearms licences, such as the Complainant, were stored on the national fingerprints database and routinely compared to those found at crime scenes across Australia. The Privacy Commissioner decided that police can use the personal information of firearms licence holders for the investigation of criminal offences.

IPP 2.1(g)(ii): the enforcement of laws relating to the confiscation of the proceeds of crime

2.127 Laws relating to the confiscation of the proceeds of crime include the *Confiscation Act 1997* (Vic) and comparable laws in other States, Territories and the Commonwealth. These laws allow for the seizure and confiscation of property and other proceeds derived from the commission of criminal offences.

2.128 In Victoria, the law which relates to the confiscation of the proceeds of crime is the *Confiscation Act 1997*. Asset Confiscation Operations is the business unit within the Department of Justice and Community Safety responsible for the confiscation and disposal of property connected to crime. The seizure and sale of personal goods or belongings derived from the commission of criminal offences is the responsibility of Victoria Police.

IPP 2.1(g)(iii): the protection of the public revenue

2.129 'Public revenue' refers to regular payments to Commonwealth, State, Territory and Local Governments, such as taxes (including excise and duties), levies, rates, application fees and charges. The term may not encompass fines enforcement, as fines are not regular payments made to a government agency. However, as discussed below, IPP 2.1(g)(v) may be a basis for use and disclosure in the fines enforcement context.

[47] *Complainant AB v Victoria Police* [2006] VPrivCmr 3.

IPP 2.1(g)(iv): the prevention, detection, investigation or remedying of seriously improper conduct

2.130 'Seriously improper' is not defined in legislation. Instead, it can be interpreted as a higher standard of misconduct proportionate and reasonable in the circumstances. 'Seriously improper conduct' may include serious breaches of standards of conduct associated with a person's duties, powers, authority and responsibilities. It includes corruption, abuse of power, dereliction of duty, and breach of obligation which warrant enforcement action from an enforcement body.

2.131 Activities or behaviours which constitute misconduct are sometimes set out in statutes that apply to specific organisations or the public service as a whole. For example, s 22 of the *Public Administration Act 2004* (Vic) lists the types of activities that are regarded as 'misconduct' by public sector employees. This includes contravention of a binding code of conduct or use of position for personal gain.

2.132 A number of statutory agencies exist to investigate allegations of serious misconduct, particularly where they concern individuals engaged in regulated professions such as teachers, lawyers and health professionals.

IPP 2.1(g)(v): preparation and conduct of court or tribunal proceedings, or implementation of the orders of a court or tribunal

2.133 Use and disclosure under this heading would include proceedings in the courts and tribunals of Victoria, other States and Territories and the Commonwealth.

2.134 Uses and disclosures of personal information to a law enforcement agency that is empowered to implement the orders of a court or tribunal need a clear link to the order that is being enforced. Any disclosure should be limited in scope to what is necessary and relevant in each case. This ground should not be used as a basis for the bulk release of information about individuals who are not subject to the orders which are being enforced.

2.135 A record of a reasonable belief the disclosure is reasonably necessary should comply with the requirements of IPP 2.2.

IPP 2.1(h): Commonwealth security agencies

2.136 IPP 2.1(h) allows an organisation to disclose information to officers of the Australian Security Intelligence Organisation (**ASIO**) and the Australian Secret Intelligence Service (**ASIS**) where the agency has requested the information in connection with its functions and:

- the disclosure is made to an ASIO or ASIS officer or employee who is authorised in writing by the Director-General of ASIO or ASIS to receive the information; and
- the Director-General of ASIO or ASIS has also certified in writing that the disclosure would be connected with the performance by ASIO or ASIS of its functions.

2.137 Organisations complying with requests from ASIO or ASIS may wish to consider keeping a record of the disclosure in case the disclosure is queried, but this is not a requirement of the PDP Act.

Verifying the authority underpinning requests for information under IPPs 2.1(f)-(h)

2.138 When dealing with a request for information or documents under IPPs 2.1(f)-(h), organisations should make sure the request is legitimate, and the requester is authorised to act on behalf of the

organisation that has the power to demand access to the information. This may entail verifying the identity and authority of the person making the request, for example, by requiring a verbal, or preferably written, confirmation from a more senior officer in the organisation. The requester should also be able to provide a specific reference to their legislative authority, for example, by stating the section in the relevant Act they are relying on to authorise or demand the information being sought.

2.139 Organisations are not authorised by IPP 2.1(g) to simply hand over information on request. IPP 2.1(g) requires the organisation to make a judgement about whether the use or disclosure is reasonably necessary in the circumstances. See *Dodd v Department of Education and Training* (General) [2005] VCAT 2207, where VCAT noted a Department may need to give more consideration to relevance when exercising a discretion to release information under IPP 2.1(g) than it might when responding to a compulsory demand for information under IPP 2.1(f):

> *It is a central plank of Dr Dodd's submissions that he considers the Department had a responsibility to consider the relevance of these two documents to the enquiry into [a fellow teacher's] conduct when making the documents available to VIT [the Victorian Institute of Teaching, regulator of the teaching profession]. While that submission might have force if one were considering IPP 2.1(g), that is not the case with IPP 2.1(f).*
>
> *Section 27(2) of the VIT Act requires the department to provide VIT with any information VIT might reasonably require to conduct its enquiry. The mandatory duty imposed on the Department is to provide information, nothing more. It does not impose a duty on the Department to consider matters such as relevance – that rests with VIT. And indeed it would be a strange state of affairs were it not so. VIT is given the power to inquire and it would be an extraordinary fetter on its task if it were only to be given the material the Department considered relevant to the task. VIT is not bound by the Department's findings; it must consider the evidence afresh and come to its own conclusion. Furthermore the remedies available to it are not identical with those provided to the Department. In my view there is absolutely no foundation for suggesting that the department should consider the relevance of documents it makes available to VIT pursuant to the obligation cast on it by section 27.*

2.140 When assessing whether to disclose information to a law enforcement agency, the organisation can take the following steps to assess whether the request is properly made.

- Consider if the information is to be released to an authorised member of a 'law enforcement agency' (as defined in s 3 of the PDP Act). Has the member's identity and authority to make the request been verified?
- Consider if the information is relevant to one of the five purposes specified in IPP 2.1(g)? Has this use been confirmed by the law enforcement agency? What information has been provided to verify the information is to be used for the stated purpose?
- Contacting the law enforcement agency to verify the request and to establish what information is being requested, so only the required information is provided to prevent making an excessive disclosure. Irrelevant third-party information should be redacted.
- Discussing the decision to disclose information with the appropriate staff within your organisation, for example, the legal department.
- Ensuring the information related to making the decision and related correspondence is stored appropriately. Refer to IPP 2.2.

IPP 2.2: Written notes of uses and disclosures under IPP 2.1(g) to law enforcement agencies

2.141 IPP 2.2 states a written note must be made of any use or disclosure made under IPP 2.1(g) to a law enforcement agency. It does not specify what should be included in the note, but the note should include information that can assist in establishing the rationale and circumstances of the disclosure, so that if this information is requested in the future, it can be retrieved and provided.

2.142 The note should specify at least the following information:

- the personal information used or disclosed, with a copy of any material supplied;
- a copy of the request for the information;
- the law enforcement agency or agencies and their representatives' names and the date that information was provided;
- the basis of the reasonable belief that the use or disclosure was reasonably necessary, taking care not to prejudice any investigation or proceeding including any supporting documentation used in making the decision to disclose the information; and
- the name and title of the decision-maker.

2.143 This information should be stored securely, especially if the information is sensitive, in accordance with IPP 4.1.

Recording uses and disclosures of information under IPPs 2.1(e)-(h)

2.144 In the PDP Act there is only a requirement to record a note if a use or disclosure is made under IPP 2.1(g), which is stated in IPP 2.2. However, decisions or queries may be made in relation to any use or disclosure under IPPs 2.1(e)-(h). Therefore, it is recommended any decision to use or disclose information under IPPs 2.1(e)-(h) be recorded, including the reasons for the decision made. For more guidance, refer to IPP 2.2 above.

> Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond 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
IPP 2 – Use and Disclosure 2019.B	Edits following consultation.	14 November 2019
IPP 2: Use and Disclosure 2019.A	Consultation draft.	28 February 2019
IPP 2: Use and Disclosure (2011)	2011 pdf version.	2011