Office of the Victorian Information Commissioner

IPP 6 – Access and Correction

Freedom of Information | Privacy | Data Protection

IPP 6 – Access and Correction

On this page

Document version: IPP 6 – Access and Correction 2019.B, 14 November 2019.

6.1 IPP 6 provides individuals with a right to access and correct their personal information. If an organisation holds personal information about an individual, it must provide the individual with access to the information upon the individual's request, except where an exception applies. If the information is inaccurate, the organisation must take reasonable steps to correct the information upon request.

6.2 IPP 6 interacts with a number of the other IPPs, namely IPP 3 (Data Quality) and IPP 5 (Openness). Allowing individuals to access and correct their personal information can help ensure and maintain the accuracy, completeness, and currency of the personal information that organisations hold as required by IPP 3. IPP 5 requires organisations to have a document setting out their policies on the management of personal information (often referred to as a privacy policy). A privacy policy lets individuals know what types of personal information an organisation generally holds, so they can specifically ask for access to that information. A privacy policy can also help individuals decide whether to make an access or correction request under IPP 6 or the *Freedom of Information Act 1982* (Vic) (**FOI Act**).

What documents does IPP 6 apply to?

6.3 The FOI Act is the primary mechanism for access to and correction of information held by Victorian government agencies. IPP 6 only applies where the FOI Act does not. The application of IPP 6 is described in the Explanatory Memorandum to the PDP Act:

> *Principle 6 provides individuals with a right to access their information and make corrections to it, where necessary. In Victoria, the Freedom of Information Act already provides a right of access to documents held by Government. The Bill does not propose to disrupt the established systems of access under this scheme by supplanting them or creating a concurrent system.*

6.4 The table below provides organisations guidance about which documents are subject to IPP 6 and which are subject to the FOI Act.

Type of organisation	Relevant access and correction pathway	Explanation
Victorian government agencies, including: • departments • councils • 'prescribed authorities' (see below)	FOI Act	A document in the possession of a Victorian government agency is subject to the FOI Act, under ss 13 and 39 of the FOI Act.[1] Section 5 of the FOI Act defines 'agency' to include departments, councils and 'prescribed authorities'.[2] As documents in the possession of these agencies are subject to the FOI Act, IPP 6 does not apply to

[1] Some documents in the possession of an agency may not be able to be accessed under the FOI Act by virtue of a provision in legislation that states the FOI Act doesn't apply – for example s 29A of the *Ombudsman Act 1973* (Vic) and s 78 of the *Protected Disclosure Act 2012* (Vic). These documents may be subject to IPP 6, to the extent that they contain personal information.

[2] See s 5 of the FOI Act for a definition of 'prescribed authority'.

		those documents.
Prescribed authorities	FOI Act	'Prescribed authorities' include body corporates established for a public purpose under an Act (excluding certain bodies), and certain persons and bodies declared by regulations to be a prescribed authority for the purposes of the FOI Act.[3] Examples of prescribed authorities include the Mental Health Tribunal, the RSPCA, Racing Victoria, and the Victorian Legal Services Board. Examples of prescribed persons and bodies include the Auditor-General, the Health Complaints Commissioner, and the Ombudsman. As documents in the possession of prescribed authorities are subject to the FOI Act, IPP 6 does not apply to those documents.
Ministers	Usually FOI	The FOI Act applies to 'an official document of a Minister, other than an exempt document'. This means that IPP 6 does not apply to official documents of a Minister. However, documents in the possession of a Minister that do not fall within the FOI Act definition of 'official document of a Minister' will be subject to IPP 6 if they contain personal information. For example, documents dealing with constituency matters.
Parliamentary Secretaries	IPP 6	Parliamentary Secretaries are not included in the definition of 'agency' under the FOI Act. Part 3 of the PDP Act applies to Parliamentary Secretaries, according to the definition of organisation in s 13 of the PDP Act. As documents held by Parliamentary Secretaries are not subject to the FOI Act, they are subject to IPP 6 if they contain personal information.
Contracted service providers (**CSPs**)	IPP 6 FOI (indirectly, via the contracting	IPP 6 will apply to documents held by CSPs where the CSP has been contractually bound to the IPPs and the document contains personal information.[4]

[3] Schedules 1 and 2 of the Freedom of Information Regulations 2019 (Vic) contain a complete list of prescribed authorities and prescribed persons and bodies. Bodies or persons may also be deemed to fall within, or outside, the FOI Act by virtue of other laws or under s 5(2)-(4) of the FOI Act.

[4] See the explanation below 'When is information 'held' by an organisation?' and s 17(2) of the PDP Act.

	(outsourcing) agency)	This is because the FOI Act does not create a direct right of access to documents held by a CSP. However, in certain circumstances, documents held by a CSP can be accessed via an FOI request to the outsourcing agency.
Courts or tribunals	FOI Act (for non-judicial documents only)	Judicial or quasi-judicial documents of courts and tribunals are not covered by the FOI Act due to s 6 of the FOI Act. This would ordinarily mean they are captured by IPP 6. However, s 14(3) of the PDP Act expressly states that documents captured by s 6 of the FOI Act are not covered by IPP 6.[5] The FOI Act *does* apply to documents of courts or tribunals that do not relate to judicial or quasi-judicial functions.[6] This means IPP 6 does not apply to these documents. Under s 6 of the FOI Act, documents or information relating to the judicial functions of courts are excluded from the FOI Act. Section 14(3) of the PDP Act also excludes these documents from the coverage of IPP 6. IPP 6 does not apply to any documents of a court or tribunal. The FOI Act applies to some.
Bodies excluded from the FOI Act by s 5(3) of the FOI Act	N/A	Some bodies are excluded from the definition of 'prescribed authority' by s 5(3) of the FOI Act. This includes 'prescribed offices', listed under reg 7 of the Freedom of Information Regulations 2019. The offices of the Director of Public Prosecutions, the Public Advocate, and the Solicitor-General are prescribed offices. Bodies that are excluded by virtue of s 5(3) of the FOI Act are not required to comply with IPP 6.[7] Neither the FOI Act, nor IPP 6, apply to documents held by these bodies.
Other bodies established or appointed for a public purpose by or under an Act, that are not covered by the FOI Act	IPP 6	Some bodies may not fall under the definition of an agency under the FOI Act, but still fall within the definition of organisation in the PDP Act. For example, in *Re Clarkson and Office of Corrections* (1989) 4 VAR 1, the Victorian Administrative Appeals Tribunal found the Adult Parole Board (APB) was not a prescribed body under the FOI Act. However, as

[5] Section 6AA of the FOI Act states that the Act does not apply to certain documents held by OVIC.
[6] FOI Act, s 6.
[7] PDP Act, s 14.

the APB is established under the *Corrections Act 1986* (Vic) for a public purpose, IPP 6 would apply.[8]

IPP 6.1: Right of access to personal information

6.5 IPP 6.1 provides individuals with a right to access their personal information, subject to limited exceptions:

> If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that [one of the exceptions in IPP 6.1(a)-(j) applies].

Providing partial or limited access

6.6 IPP 6 permits organisations to refuse access only to the extent that one of the exceptions in IPP 6.1 applies. As such, where an organisation is proposing to withhold personal information because one of the exceptions in IPP 6.1(a)-(j) applies, it should consider to what extent access can be provided. This may involve using mutually agreed intermediaries under IPP 6.3. Or, it may involve providing access to documents after removing (or redacting) material that would be subject to one of the exceptions in IPP 6.1(a)-(j). If an exception in IPP 6.1 only applies to parts of the information that are requested, the other parts should be released.

6.7 Organisations proposing to rely on an exception should also consider whether access can be granted subject to conditions that would remove the grounds for the exception. Examples of conditions that could be applied include:

- an undertaking not to further disclose the information or not to use the information except for specified purposes;
- redacting information that falls under an exception;
- only allowing the information to be inspected in person, without copies or notes being taken.

6.8 IPP 6 does not stipulate how access is to be given – whether through a right of inspection, copies of records containing the personal information, or records in digital form. As a matter of best practice, organisations should attempt to provide access in the form requested. However, the requirements of IPP 6 can be met by providing access in another form, where providing the information in the form requested is impossible or inappropriate.

When is information 'held' by an organisation?

6.9 An organisation is required to provide access to personal information it 'holds'. Under s 4(1) of the PDP Act, an organisation holds personal information 'if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria.' In an outsourcing context, this means IPP 6 can apply to the personal information 'held' by a CSP, if the

[8] PDP Act, ss 13(1)(e), 20.

outsourcing government organisation can 'control' that information.

6.10 If an organisation receives a request for access but the information does not exist or cannot be found, access can be refused. However, when refusing access to information that cannot be found, the organisation should be able to demonstrate that reasonable searches for the information occurred.

IPP 6.1 Circumstances in which access can be refused

6.11 The exceptions limiting the right of access under IPP 6 are listed in IPP 6.1(a)-(j). Access may be refused to the extent that one of these exceptions applies.

6.12 Many of the terms in IPP 6.1(a), (f), (g) and (i) are discussed elsewhere in these Guidelines. For example:

- 'serious threat' (IPP 6.1(a)) is discussed under IPP 2.1(d);
- 'lawful' (IPP 6.1(f)) is discussed under IPP 1.2;
- 'Required or authorised by law' (IPP 6.1(g)) is discussed under IPP 2.1(f);
- Many of the concepts in IPP 6.1(i) and (j) relating to law enforcement matters and national security are discussed under IPP 2.1(g) and IPP 2.1(h) respectively.

IPP 6.1(a): Access would pose a serious threat to the life or health of any individual

6.13 The exception in IPP 6.1(a) permits an organisation to withhold access to information where access would pose a serious threat to the life or health of any individual. The term 'serious threat' is considered in relation to IPP 2.1(d).

6.14 Organisations that deny access should be able to provide evidence as to how the access to the material would pose a threat to the life or health of an individual. Organisations may also need to consider whether the use of an intermediary (under IPP 6.3) would overcome any serious and imminent threat to the life or health of an individual. In *D v Charitable Organisation* [2011] PrivCmrA 4, the organisation was concerned that providing access to personal information posed a threat to the safety or health of the complainant. This threat was overcome by providing the information via a health practitioner, who could support the complainant while providing them with the requested information.

IPP 6.1(b): Impact on another person's privacy

6.15 IPP 6.1(b) permits organisations to refuse access if access 'would have an unreasonable impact on the privacy of other individuals'. This exception is similar to s 33 of the FOI Act which exempts documents, or parts of documents, from disclosure to protect the privacy of other people.

6.16 Under both the FOI Act and IPP 6, the exemption is not absolute. Organisations can decide to release personal information of a third party where the access would not have an 'unreasonable impact' on the third party's privacy.

6.17 Organisations should consider whether the privacy of a third party may be adversely impacted by the disclosure of his or her information before releasing information about a third party.

6.18 Under s 33(2B) of the FOI Act, in determining whether disclosure of a third party's personal information would be unreasonable, agencies must consult with the third party and seek their views about the proposed disclosure. There is no equivalent obligation under IPP 6 to notify individuals of a

proposed release of their information.

6.19 In some cases, it will be clear from the material that disclosure may have an unreasonable impact on the third party's privacy. In others, it may be necessary to consult the third party to decide if disclosure would be unreasonable.

6.20 Before refusing a request for access to information based on IPP 6.1(b), organisations should consider the following questions:[9]

- Can the information can be provided in a form that removes identifying information of the third party?
- Can consent be sought from the third party to release their personal information?
- Was the information about the third party provided to the agency by the person who is now requesting the information? If so, it is unlikely providing the information back to the individual who gave it to the agency would be an unreasonable impact on the third party's privacy.

6.21 Redaction can be a solution. For example, in *C v Insurance Company* [2006] PrivCmrA 3, the Australian Privacy Commissioner found that releasing some documents in response to the access request would have an unreasonable impact on a third party's privacy. The Commissioner requested the organisation redact the information in the documents that would cause the unreasonable impact before releasing the documents.

6.22 In *Case note 277412* [2016] NZ PrivCmr 13, an organisation refused access to footage, on the basis that it was too onerous to protect the privacy of the third parties. The New Zealand Privacy Commissioner agreed with the organisation that the unedited footage would identify staff, but found the Department had not demonstrated it would be too onerous or costly to edit the footage to protect the privacy of its staff and also enable the individual to access the footage.

IPP 6.1(c): Frivolous or vexatious requests

6.23 Access can be restricted under IPP 6.1(c) where a request is frivolous or vexatious. The ordinary dictionary meaning of 'vexatious' is 'not having sufficient grounds of action and seeking only to annoy'.

6.24 A request should not be refused on this ground unless there is a clear and convincing basis for deciding a request is frivolous or vexatious. For example, it is not a sufficient basis that a request would cause inconvenience or irritate an organisation.

> **Case Study 6A: Access request not vexatious[10]**
>
> An employee requested access to personal information held by his employer after a dispute involving the use of a company vehicle. The company refused his request under the New Zealand *Privacy Act 1993* because it was vexatious. The employee complained to the New Zealand Privacy Commissioner.
>
> The company decided the request was vexatious because, at the time, it was in the middle

[9] See also Office of the Australian Information Commissioner, APP Guidelines, Chapter 12: APP 12 — Access to personal information, paragraph 12.38.
[10] *Employee's access request considered "vexatious" by employer (Case Note 18109)* [1999] NZPrivCmr 14.

of significant industrial action, coordinated and supported by a trade union, and the union had encouraged members to make mass requests for access under the *Privacy Act 1993* (NZ).

The Privacy Commissioner suggested that, for a request to be refused on the ground it is vexatious, 'the requester must be believed to be patently abusing the rights of access to information, rather than exercising those rights in a bona fide manner'. The request must be considered in light of the surrounding circumstances.

The Privacy Commissioner decided the employer had not considered all the circumstances surrounding the employee's request, having apparently relied on the timing of the request to determine it was part of the industrial action. The access request was influenced by the employee's dispute over the company car, which was unrelated to the industrial action. The request appeared to be bona fide and made in good faith. Therefore, the employer did not have a proper basis to withhold access to the information from the employee.

IPP 6.1(d): Information relating to existing legal proceedings between organisation and individual

6.25 IPP 6.1(d) serves a similar purpose as s 32 of the FOI Act (documents affecting legal proceedings). IPP 6 is not intended to interfere with existing procedures for discovery in legal proceedings. An organisation may withhold information which relates to existing legal proceedings between the organisation and the individual, where the information would not be accessible by the process of discovery or subpoena in those proceedings.

IPP 6.1(e): Providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations

6.26 IPP 6.1(e) applies where the information requested may reveal or compromise the negotiating strategy of an organisation when it is negotiating with the individual requesting the information.

6.27 This ground might apply when an organisation is:

- negotiating the settlement of a claim brought by an individual for compensation (for example, for negligence or wrongful dismissal), and releasing the personal information may reveal the organisation's strategy to settle or defend the claim; or
- engaged in a commercial negotiation with a potential supplier who is an individual, where releasing the information requested may reveal how much the organisation would be able to pay the individual.

IPP 6.1(f): Providing access would be unlawful

6.28 IPP 6.1(f) allows an organisation to refuse access to a document where providing access to the document would be unlawful.

6.29 The core meaning of 'unlawful' is activity that is criminal, illegal or prohibited by law. Examples of unlawful activity include criminal offences, unlawful discrimination or harassment, and trespass. It does not include breach of contract. For example, this ground might apply where giving access would be a breach of confidence or a breach of copyright. It may also apply where a statutory 'secrecy provision' prohibits disclosure of certain information.

IPP 6.1(g): Denying access is required or authorised by law

6.30 This ground applies where an Australian law, or court or tribunal order, forbids the disclosure of information, or a law or order authorises or confers discretion on an organisation to refuse a request for access to the information. There is overlap between this ground and IPP 6.1(f), 'providing access would be unlawful'.

IPP 6.1(h): Prejudice an investigation into possible unlawful activity

6.31 IPP 6.1(h) allows an organisation to refuse access where it might prejudice an investigation of possible unlawful activity. This enables organisations to investigate unlawful activity, such as theft or fraud, without an access request compromising the investigation. This exception should be narrowly applied to information that is part of the investigation into possible unlawful activity. It should not be applied broadly to any information that relates to an investigation.

6.32 In some situations, even revealing the existence of an investigation may prejudice it. As such, organisations may sometimes need to refuse a request without advising of the precise exception that was relied on and will only be able to provide very general reasons for refusing access. Organisations may wish to consider providing a response that neither confirms nor denies whether the requested information is held.

IPP 6.1(i): Prejudice law enforcement activities

6.33 IPP 6.1(i) resembles s 31 of the FOI Act. It guards against prejudice to law enforcement activities. It applies where the release of the requested information would prejudice certain functions carried out by, or on behalf of, a law enforcement agency. The functions protected by IPP 6.1(i) 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 public revenue;
- the prevention, detection, investigation or remedying of seriously improper conduct; and
- the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders.

6.34 As with IPP 6.1(h), the exception in IPP 6.1(i) does not apply to all information that relates to these activities. The release of the information must be *likely to prejudice those activities*.

6.35 Examples of the sorts of information to which access may be refused under this exception includes information that reveals:

- the identity of a confidential source or informer;
- the existence of an investigation that is being conducted in private; and
- the steps that a law enforcement body takes to detect unlawful behaviour, which if disclosed would be less effective.

IPP 6.1(j): Security of Australia

6.36 IPP 6.1(j) is intended to protect the national security interests of Australia, by providing an exception for disclosures where ASIO, ASIS, or a law enforcement agency request that the document not be released. It is similar to the national security exemption in s 29A of the FOI Act.

6.37 Where the request comes from a law enforcement agency, organisations should consider the basis for the request. The request must be related to a 'lawful security function' of the agency, which will

encompass investigations into terrorism offences, but it would not extend to the investigation of ordinary criminal offences that do not involve some element of national security. In those cases, IPP 6.1(i) may be more relevant. It may be useful to consult *Verifying the authority underpinning requests for information under IPPs 2.1(f)-(h)* if the request for information is from a law enforcement agency.

IPP 6.2: Commercially sensitive decision-making

6.38 IPP 6.2 allows organisations to give individuals an explanation for a commercially sensitive decision, rather than providing direct access to the information underpinning that decision. This may be done where providing the information would reveal evaluative information generated in connection with the decision-making process.

6.39 IPP 6.2 cannot be used to withhold factual personal information on which a commercial decision is based – only 'evaluative information'. IPP 6.2 seeks to ensure that, where individuals are adversely affected by a commercial decision, they are able to receive an explanation of the reasons for the decision, rather than being refused access to the information.

IPP 6.3: Providing access through an intermediary

6.40 Where one of the exceptions in IPP 6.1(a)-(j) applies, IPP 6.3 requires organisations to consider the use of an intermediary to allow sufficient access to meet the needs of both parties.

6.41 As stated earlier, an organisation should endeavour to provide access to the extent it can. Where the organisation decides full access to the requested information should not be granted because a relevant exception applies, the organisation should try to provide more limited access. IPP 6.3 intends to provide organisations with an alternative to a complete denial of access by using 'neutral parties' to convey the requested information to the applicant. The information may be provided either in full or in part by the intermediary.

6.42 An example of a situation where access could be given through an intermediary is where the organisation is concerned an individual will harm themselves if they receive the information in question. In Australian Privacy Commissioner, *'LS' and 'LT'* (Privacy) [2017] AICmr 60 (26 June 2017), a patient of a psychiatrist sought access to her medical records after her relationship with the psychiatrist broke down. The psychiatrist refused access to the records as she was concerned the patient would harm herself if she saw them. After considering evidence from the psychiatrist and the patient's new treating doctor, the Commissioner decided access must be given through an intermediary psychiatrist, who would interpret and explain the records to the patient in a way that would minimise any risk of self-harm.

6.43 The use of an intermediary will not be appropriate in circumstances where any form of access will result in the harm the relevant IPP 6.1 exception is attempting to prevent. For example, where disclosure is likely to prejudice law enforcement activities by revealing the existence of an ongoing investigation, it is unlikely access through an intermediary will address this concern.

6.44 When an organisation has decided to use an intermediary, the organisation should consider the following questions.

- Will the intermediary be acceptable to both the individual seeking access to information and the organisation?

- Does the intermediary have the relevant skillset or knowledge required in the circumstances? An appropriate intermediary might be a family member, a medical practitioner or a legal representative.
- Do the organisation, the intermediary and the individual have a common understanding of the role of the intermediary and how access will be provided?

6.45 If the organisation decides not to proceed with using an intermediary, it will need to provide reasons for refusing access under IPP 6.7.

IPP 6.4: Access fees

6.46 Section 119 of the PDP Act allows organisations to charge a 'prescribed fee' for providing access under the PDP Act. IPP 6.4 permits the organisation to refuse access until the prescribed fee is paid. Regulations prescribing fees for access can be made by the Governor in Council under s 125(2) of the PDP Act.

6.47 As of October 2019, no regulations have been made and there is no 'prescribed fee'. This means organisations cannot charge fees under s 119 and must provide access to personal information free of charge.

IPP 6.5: Right of correction

6.48 If an individual establishes the information held by an organisation about him or her is not accurate, complete or up to date, IPP 6.5 requires the organisation to take reasonable steps to correct the information.

6.49 Providing individuals with a right of correction helps to ensure organisations do not act on wrong information or misrepresent personal facts about individuals. Inaccurate information can negatively impact individuals about whom decisions are later made. A right of correction helps maintain the data quality of their information, complementing IPP 3.

6.50 Organisations can correct personal information by deleting, amending or adding to a record. Generally, the organisation should retain both the old and new information to ensure they meet any record-keeping obligations under the *Public Records Act 1973* (Vic). However, old information should be clearly marked as no longer current. The date and reason for the correction of the information should be included in the records. This enables the organisation to track changes made to the information for audit and complaint handling purposes.

6.51 If the organisation and the individual cannot agree on whether the information is accurate or not, where requested by the individual, the organisation must, under IPP 6.6, take reasonable steps to associate the relevant information with a statement saying the individual claims the information is not accurate, complete or up to date. This is discussed further below.

IPP 6.6: Disagreement regarding accuracy of information

6.52 IPP 6.6 states:

> If the individual and the organisation disagree about whether the information is accurate, complete and up to date and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.53 An organisation considering attaching such a statement to information should first assess whether or not the personal information in question is complete, accurate, and up to date. If the organisation agrees with the individual that the record needs correcting, the organisation should correct the information in accordance with IPP 6.5 (as above).

6.54 However, where the individual requesting the correction and the organisation disagree, the individual may make a request for a statement to be attached to the information conveying the individual's opposing view. This does not prevent the organisation from offering to attach a statement to the information in an effort to resolve a dispute regarding the correction of information.

6.55 An organisation can attach a statement requested under IPP 6.6 in multiple ways. For example, the organisation could:

- placing a file note on the record;
- include the statement in a related record; or
- indicate that there is a statement linked to the information and the location of that statement.

6.56 The organisation should ensure it is clear to anyone who accesses the information that the accuracy is disputed and the reason why the organisation has decided not to correct, delete or add the information as requested by the individual.

IPP 6.7: Reasons for denial of access or refusal to correct

6.57 Where an organisation refuses a request for access or correction, IPP 6.7 requires the organisation to provide reasons for its decision.

6.58 Additionally, an organisation must provide reasons for its decision to:

- refuse a request for access because one more of the exceptions under IPP 6.1 applies;
- refuse to make an amendment, because information is accurate, complete and up to date; or
- refuse to amend information because to correct information by completely removing information would be contrary to proper records management practices and harm the integrity of the file.

6.59 When an organisation provides reasons for refusal of access or correction of information, it should:

- provide the grounds for refusal to provide access or correct the information as requested;

- if appropriate, clearly state any steps that the individual may take in order to facilitate the access or correction, such as re-framing their request or changing its scope; and
- state the individual's right to complain to OVIC if the individual disagrees with the organisation's decision.

6.60 In limited circumstances, it may be inappropriate to provide detailed reasons for denying access to information. In these cases, the organisation will only be able to provide very general reasons for refusal or may decide to neither confirm nor deny the existence of a document that has been requested. For example, in situations involving family violence, an organisation may feel it is more appropriate to neither confirm nor deny the existence of certain records. Providing reasons for refusal of access to the individual may not be appropriate if the individual is able to infer they are the subject of a family violence investigation.

IPP 6.8: Time limit for responding to request for access or correction

6.61 IPP 6.8 sets a time limit for organisations to respond to a request for access or correction. Organisations must respond to a request as soon as practicable, but no later than 45 days after receiving the request.

6.62 Organisations should endeavour to provide access or agree to correct, or provide reasons for a denial of access or refusal to correct, within this time limit. If it is impossible for an organisation to finalise the processing of a request within 45 days, it should at least provide reasons for delay to the person requesting access under IPP 6.8(c).

Who is entitled to exercise the rights of access and correction under IPP 6?

Access to and correction of one's own information

6.63 The right of access and correction under IPP 6 can only be exercised by the person whose information is contained in the record. However, if that person is incapable of making a request for access or correction, an authorised representative may make the request on that person's behalf.[11] The role of authorised representatives in making decisions on behalf of others is discussed in the Key Concepts under Capacity.

6.64 IPP 6 only requires an organisation to provide access to 'personal information' as defined by the PDP Act, see Key Concepts: Personal Information. In contrast, the right of access under the FOI Act is wider than IPP 6. The FOI Act right of access it is to any 'document' of an agency, not only personal information.[12]

6.65 Organisations must ensure the person applying for access is actually who they say they are. An individual may attempt to use IPP 6 to access information about another individual by impersonating that person. Organisations should establish an individual's identity before providing access. Failure to do so or providing access to the wrong person could breach IPP 4.1 (Data Security).

Accessing a child's personal information

6.66 Children and young people are entitled to seek and correct their own information where they are

[11] PDP Act, s 28(2).
[12] FOI Act, s 13.

capable of understanding the general nature and effect of making a request to access or correct their personal information. Where they are incapable of understanding the nature and effect of such a request, an authorised representative (such as a parent) can make the request on their behalf under s 28(2) of the PDP Act. See also Capacity, consent and mature minors in the Key Concepts chapter.

6.67 An access request made under IPP 6 by a parent or other authorised representative must be done on behalf of the child. It must not be motivated by the parent's own interests. VCAT has considered the legitimacy of a father's request for access to his daughter's file under Health Privacy Principle 6 of the *Health Records Act 2001* (Vic). The father asserted he was entitled to the file as the child's parent and guardian. However, VCAT found the father had no independent right of access to his child's records, nor did he have standing to bring a complaint when he was denied access.[13]

> 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 6 – Access and Correction 2019.B	Edits following consultation.	14 November 2019
IPP 6: Access and Correction 2019.A	Consultation draft.	1 August 2019
IPP 6: Access and Correction (2011)	2011 pdf version.	2011

[13] *Callanan v McLoughlan (General)* [2006] VCAT 1099.