Information Privacy Principles and Child Protection

Purpose

South Australian Government agencies are required to comply with Premier and Cabinet Circular No 12; more commonly known as the *Information Privacy Principles (IPPs) Instruction (Instruction).* The IPPs guide the collection, storage, use and disclosure of personal information by State Government agencies.

The purpose of this Information Sheet is to provide an outline as to how the IPPs work with existing laws and policies to promote the protection of children and young people.

Child Protection

The IPPs should not represent a barrier to the collection, use or disclosure of information necessary to promote the protection of children and young people.

The IPPs recognise that privacy is not an absolute right and must be balanced against other important rights and interests. This includes the right of children to be protected from harm. There are a number of important laws and government policies that work to promote child protection and it is important for agencies and their staff to understand how the IPPs work with those laws and policies.

Children's Protection Act 1993

The Instruction does not affect a person's obligation to report a reasonable suspicion of abuse or neglect under Section 11 of the *Children's Protection Act 1993*. Under section 11, certain persons, such as teachers, police officers and medical practitioners, must notify the Child Abuse Report Line (CARL) if they suspect on reasonable grounds that a child has been or is being abused or neglected. Section 11(2) of the Act provides a list of persons that are required to report abuse or neglect.

IPP 10(d)[1] permits the disclosure of personal information for a purpose that is not the purpose of collection where the disclosure is required or authorised under law. Notification of abuse or neglect under Section 11 of the *Children's Protection Act 1993* is required by law.

Reports are to be made to CARL by calling 131478 as soon as the relevant person forms a suspicion of child abuse or neglect.

[1] A reference to a particular IPP in this Information Sheet is a reference to the relevant subclause under Clause 4 of the Information Privacy Principles Instruction.

Information Sharing Guidelines for Promoting Safety and Wellbeing (ISG)

The *Information Sharing Guidelines for promoting safety and wellbeing* (ISG) are authorised by a Cabinet Direction. The ISG are designed to give providers of services to children, young people and adults, confidence in sharing information where there are threats to safety and wellbeing.

The ISG aligns with the intent of the IPPs by providing a practical framework and step by step process to appropriate information sharing practice. Together, the IPPs and ISG define both the principles and practice for disclosing personal information.

For those applying the ISG, the need for information sharing arises where there is reasonable suspicion that individuals or groups are at risk of harm and it is believed information sharing can support effective service intervention. The ISG promotes privacy by prescribing information sharing and record keeping processes that are secure, timely, accurate and relevant and, importantly, that informed consent for the disclosure is sought wherever safe and possible. When it is unsafe or impossible to seek consent and the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of a person, personal information may be disclosed. This is consistent with IPP 10(c).

In following the ISG process, agencies can be confident they will meet their obligations under the IPPs. A copy of the ISG can be downloaded from the website of the South Australian Ombudsman.

The Information Privacy Principles

Collection

Under IPP 2 there are a number of basic things that an agency must tell an individual before collecting that individual's personal information. They include the purpose for collecting the information, whether the collection is authorised or required by law and the agency's usual practices in terms of disclosure.

Under IPP 3, an agency should not collect personal information that is inaccurate, irrelevant, out of date, incomplete or excessively personal. It is important that the information relied upon by agencies is as accurate and up to date as possible. Poor information quality can lead to errors and poor decision making. In the child protection context this can be particularly problematic; out-dated or incorrect address information could put a child at risk. Incomplete or inaccurate information also raises the potential for mistaken identity which could affect an individual's reputation.

Storage

Under IPP 4 an agency should take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused.

The security of information in the child protection context is vital. Information held in the course of delivering child protection and related children's services is often highly sensitive personal information. It is important that the steps an agency takes to secure this information are proportionate to its sensitivity. The consequences of the misuse, loss or unauthorised access to personal information can be very serious, particularly for victims of

Case Study:

An agency was making changes to their office and sent a number of filing cabinets for salvage via public auction. A confidential client file was left in one of the cabinets and found by the purchaser. The purchaser provided the file to a media outlet. The file included sensitive information about child protection matters.

abuse and violence. Security includes the physical security of the information and the management of access to it. Agencies need to consider how they manage information from collection through to disposal.

Agencies should ensure that their information systems maintain standards of information security proportionate to the sensitivity of the information; this includes ensuring appropriate classification of information. Standards for the security of information systems are outlined in the Government's *Information Security Management Framework* (ISMF). Agencies are required to comply with the ISMF and any information security procedures developed by their agency. The appropriate security classification for the information shared in relation to child protection is likely to be 'Sensitive: Personal' or 'Sensitive: Medical'. Marking documents with a security classification helps staff to understand the value of the information and reduces the likelihood of it being misused. Agencies can seek further advice regarding information security from their Agency Security Adviser or their IT Security Adviser.

Use and Disclosure

The IPPs provide for the use and disclosure of personal information for the purpose it was originally collected for (the primary purpose), or for another related purpose that would be reasonably expected by the person to whom the information relates. Information is sometimes used or disclosed in the child protection context for purposes that would not have been expected when it was collected. Such secondary use or disclosure should only normally occur with the consent of the person to whom the information relates. However, in some circumstances it is not reasonable or practicable to seek consent; in fact it may not be safe to do so. The IPPs include a number of provisions that permit the use or disclosure in these circumstances including where:

- reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person
- required or authorised by law
- reasonably necessary for the enforcement of the criminal law or to protect the State as an employer
- the agency is investigating or reporting suspected unlawful activity
- the information relates to illegal conduct or serious misconduct in relation to a person and the disclosure complies with any applicable Ministerial guidelines.

Case Study:

The police are aware that a male with a history of child sexual assault convictions has begun to cohabitate with a single mother of two girls, aged 8 and 12. The mother may or may not be aware of the male's history. She may or may not be leaving her children in the unsupervised care of the male. It is reasonable for the police to believe that it is necessary to disclose this information to the mother to prevent a serious threat to the health and safety of the children.

Serious Threats to Life, Health or Safety

The IPPs provide for the use and disclosure of information when it is apparent to an agency that it is necessary to prevent or lessen a serious threat to the life, health or safety of a person (subclause (c) of IPPs 8 and 10). Such a threat no longer has to be 'imminent' for the agency to use or disclose the personal information.

Subclause (c) of IPPs 8 and 10 permit agencies to take steps early, where necessary, to prevent or lessen

serious threats rather than waiting until the threat has actually materialised in harm to a child or young person. If applying subclause (c) agencies should consider the ISG, which provides a practical framework for making decisions to use or disclose information to prevent such harm.

Required or authorised by law

The IPPs do not override specific legal obligations of agencies relating to the use and disclosure of information. Subclause (d) of IPPs 8 and 10 permit the use or disclosure of personal information for a purpose that is not the purpose of collection where the disclosure is required or authorised under law.

If the agency is required by law to use or disclose personal information it has no choice in the matter and must do so. If an agency is authorised to use or disclose personal information it means it can decide whether or not it does so.

Reasonably necessary for the enforcement of the law

The IPPs permit an agency to use and disclose information when cooperating with law enforcement agencies or fulfilling their own law enforcement functions. This is provided for under subclause (e) of IPPs 8 and 10. Subclause (e) permits an agency to use or disclose personal information where the use or disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty.

The enforcement of the criminal law means:

- the process of investigating crime and prosecuting criminals, and
- gathering intelligence about crime to support the investigating and prosecuting functions of law enforcement agencies.

The proper protection of children and young people will rely on the cooperation of many agencies and law enforcement authorities. This could, for example, include the disclosure of information by a public school to SA Police (SAPOL) to support an investigation into child abuse. It may mean the disclosure of information by a public housing authority to SAPOL or the Department for Correctional Services about a person undergoing home detention.

Investigating or Reporting Suspected Unlawful Activity

The IPPs do not prevent an agency from investigating or reporting a suspected unlawful activity. Subclause (f) of IPPs 8 and 10 permit agencies to use and disclose personal information when investigating or reporting unlawful activity that has been, is being, or may be engaged in. This allows use or disclosure to be a necessary part of the agency's investigation into the unlawful activity or in reporting the agency's concerns to a relevant person or authority.

In the child protection context, this could include, for example, the investigation of suspected sexual assault or misconduct by an agency staff member or contractor. A relevant authority or person could include a law enforcement agency or the registered body of a relevant profession. A relevant person could also be a parent in relation to suspected unlawful behaviour at a public school where there was a risk that the parent's child could have been harmed by the suspected unlawful activity.

Illegal Conduct or Serious Misconduct in Relation to a Person

On 5 August 2013, IPPs 8 and 10 were amended to include a new subclause (g) to permit the use and disclosure of information about an individual that might reveal that

the individual has engaged in, or may engage in, illegal conduct or serious misconduct in relation to a person. Such conduct could include illegal or serious misconduct in relation to a child or young person. An agency can only use or disclose the information where they reasonably believe the use or disclosure is appropriate in the circumstances; and it complies with guidelines to be issued by the Attorney-General. These guidelines are still in development and subclause (g) cannot be utilised until they have been issued.

Where do I get more information?

This Information Sheet has been issued by the Privacy Committee of South Australia. The Committee exists to:

- advise on measures that should be taken to protect personal information
- refer written complaints received about breaches of privacy to the relevant authority
- consider agency requests for exemption from compliance with the IPPs.

Further information about the IPPs is available at www.archives.sa.gov.au.

Use of this Information Sheet

This Information Sheet is provided for general guidance to agency officers only and should not be constituted as legal advice. Agencies may need to seek formal legal advice on the application of the IPPs to their particular situation.

Need further assistance?

Contact
Tel (+61 8) 8204 8786
Email staterecords@sa.gov.au
Web www.archives.sa.gov.au

Date approved	Approved by	Date for review	Version
20/02/2019	Manager, Policy and Legislation	20/02/2020	1.1