Government of South Australia

Office of the Guardian for Children and Young People

# Submission to the Senate Public Finance and Public Administration Committee

## Australian Privacy Principles – Exposure Draft

## July 2010

To: Committee Secretary
Senate Standing Committee on Finance and Public Administration
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

From: Pam Simmons
Guardian for Children and Young People

Level 4 East, 50 Grenfell St. Adelaide
www.gcyp.sa.gov.au

Ph. 8226 8570
Email: pam.simmons@gcyp.sa.gov.au

# 1 Introduction

1.1 The position of Guardian for Children and Young People was established in an amendment to the South Australian *Children's Protection Act 1993* passed on 1 December 2005.

1.2 The Office of the Guardian for Children and Young People (GCYP) promotes and protects the rights of all children and young people under the age of 18 years in alternative care. This includes those who are in relative or kinship care, foster care, residential care or secure custody. We work to improve services to children and young people in out-of-home care, to promote and protect their rights and to strengthen their voice. To do this we work in partnership with children and young people, their families and carers, government agencies and non-government organisations (NGOs).

1.3 The Office of the Guardian is an independent government agency and the Guardian advises the Minister for Families and Communities.

1.4 We welcome the review of the Australian Privacy Principles (APPs) and proposed redrafting and updating of the structure of the *Privacy Act 1988* (the Privacy Act). Thank you for the opportunity to comment on the exposure draft. We are optimistic that clear and easily understood APPs, when consolidated into a new Privacy Act, will protect privacy and provide a robust and workable regulatory framework.

1.5 This submission will respond to those proposed amendments relevant to our functions and role, and that have significant impact on the work of this office.

# 2 Context

2.1 GCYP supports a single set of privacy principles applying to both the public and private sectors that will simplify obligations in relation to compliance with the Privacy Act. This is of particular concern for this office within the context of our experience monitoring the state-wide implementation of the South Australian Government's *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families* (ISG). (see: http://www.gcyp.sa.gov.au/information-sharing-guidelines/ )

2.2 The ISG is an early intervention strategy. It promotes a consistent approach to disclosure of personal information to assist agencies to better coordinate their efforts to support vulnerable families where there is a serious risk of harm or abuse to children, young people and their families or a risk to public safety.

2.3 The ISG followed recommendations to improve information exchange about children at risk in Robyn Layton QC (2003) *A State Plan to Protect and Advance the Interests of Children*, the Hon Justice EP Mullighan (2008) *Children in State Care Commission of Inquiry* and reports of the Child Death and Serious Injury Review Committee. Information sharing is a key element of the *Intervention Orders (Prevention of Abuse) Act 2009* and the South Australian *Family Safety Framework.*

2.4 Protocols for sharing information impact on the implementation of the COAG *National Plan to Reduce Violence Against Women and Their Children*, and the COAG *National Framework for Protecting Australian's Children 2009-2020* which commits to improving information sharing between NGOs and government agencies.

2.5 In 1992, the State Government of South Australia issued a set of Privacy Principles to regulate the way personal information can be collected, used, stored and disclosed. These principles apply only to the South Australian public sector and are administered by the South Australian Privacy Committee.

2.6 In October 2008 South Australian Cabinet endorsed the ISG to apply to the public sector and relevant NGOs that have funding contracts with the State Government. The Privacy Committee of SA granted an exemption in relation to the South Australian *Information Privacy Principle 10(b) – Disclosure of Personal Information*. The exemption removed the word 'imminent' from the IPP so that information could be shared earlier where there is risk of serious harm. The exemption is conditional upon meeting the requirements for appropriate information sharing practice (as defined by the ISG), recording of decisions, and induction conducted by all government agencies and NGOs implementing the ISG. This work is being led by this office.

## 3 South Australian Information Sharing Policy

3.1 Legal advice received by two NGOs participating in the first stage of implementation of the ISG identified inconsistencies between Commonwealth legislation and the ISG regarding release and disclosure of client information. The Commonwealth *Privacy Act 1988* applies a test of imminence to disclosure. The ISG has a pro-disclosure requirement and does not require that risk be imminent for disclosure to be justified. The ISG promotes disclosure when risk is serious and anticipated.

3.2 The ISG is being implemented across all relevant government agencies and some 600 NGOs that have a funding contract with the South Australian Government.

3.3 Incompatibility between the Privacy Act and the ISG is likely to be a serious impediment to fully implementing this South Australian Government policy. NGOs with both Commonwealth and State funded services are contractually bound by conflicting privacy and information sharing requirements.

3.4 The incompatibility poses a risk that NGOs may not intervene when there is a serious risk of harm because of confusion about what protocol (State or Commonwealth) applies or whether or not a threat must be 'imminent'.

3.5 The Australian Law Reform Commission *Report 108* claimed the test of 'imminence' can be too restrictive and prevents early intervention by services to prevent harm. The *Australian Government First Stage Response* to *Report 108* agreed, noting at the same time it is important to safeguard against the mishandling of personal information. The ISG protocol requires agencies and organisations to use or disclose personal information only after consent has first been sought, where it is safe and possible to do so. The ISG also describes when sharing of information without consent is justified and how this should be done.

3.6 Guidance on the operational application of Australian Privacy Principles (APPs) is important in assisting agencies and organisations to understand their obligations. The ISG is an appropriate framework for the use, collection and disclosure of personal information and could be used as a template by the Commonwealth Privacy Commissioner in guiding agencies in appropriate information sharing practice. Because of the strong concordance between the

ISG and the proposed APP 6, South Australian NGOs should have added confidence to implement the ISG and meet all contractual obligations with regard to protecting privacy. Legal advice to this office on the proposed amendment says NGOs implementing the ISG would be protected by the proposed Principle.

3.7 It is likely, and in some cases actual, that similar provisions for sharing information when serious harm can be anticipated but not imminent will be introduced to protect other vulnerable population groups. For example on 30 June 2010 South Australia's *Mental Health Act 2009* commenced. Section 106(2)(e) allows for 'disclosing information if the disclosure is reasonably required to lessen or prevent a serious threat to the life, health or safety of a person, or a serious threat to public health or safety'. Mental health services will implement this clause by following the ISG and their related organisational policies and procedures.

## 4 Comments about specific draft APPs

| | |
|---|---|
| 4.1 | APP 3 – collection of solicited personal information |
| | **The proposed principle is supported (in principle - pending clarification)** |
| | APP 3(1) and (2) are supported in principle.<br>The collection of solicited personal information when 'reasonably necessary' or 'directly related to function and activity' requires clearer definition, and advice and direction with particular regard to relevance and accuracy.<br>APP 3(b) is supported in principle.<br>It is necessary to provide guidance to determine 'reasonable' and 'necessary' with particular regard to relevance and accuracy. Whatever personal information is collected must be proportionate to the purpose for collection and not provide unnecessary detail. Guidance is required to assist in determining if it is safe or possible to seek consent.<br>The security of personal information as reflected in APP 11(1) should be referenced within this principle. |
| 4.2 | APP 4 – receiving unsolicited personal information |
| | **The proposed principle is supported (in part - pending clarification).** |
| | APP 4(1)(a) and (b), (2), (3), and (4)(a) are supported.<br>The benefit of APP 4(4)(b) is unclear and creates confusion about what constitutes 'personal information'. If the desired outcome is to ensure personal information is de-identified, or prevented from, at some time in the future, being identifiable, then it is unclear. |

4.3

| APP 5 – notification of the collection of personal information |
|---|
| **The proposed principle is supported (in part - pending clarification).** |
| Guidance about 'reasonable in the circumstances' is required. For organisations that are provided personal information as enabled under APP 3(3)(b) and use or disclose under APP 6(2) a risk assessment is required to determine if notification or the seeking of consent is safe, reasonable, and appropriate. In the absence of guidance and assessment, notification of the collection of personal information may exacerbate risk to health or safety. This could include workers, the individual who owns the personal information, those they relate to, or pose risk to public health or safety. Before seeking consent, or notifying collection or disclosure of personal information, consideration should be given to the likelihood an individual may:<br>• move himself/herself and his/her family out of the agency's view<br>• cease to access a service seen to be necessary for the client's or his/her children's safety or health<br>• coach or coerce family members to 'cover up' harmful behaviour to himself/herself or others<br>• abduct someone or abscond<br>• assault or threaten to assault others<br>• attempt suicide<br>• destroy incriminating material relevant to a person's safety<br>• pose a risk to themselves or to public safety<br>Where safe to do so, seeking informed consent for collection or disclosure of personal information is the preferred approach. Providing advice at the point of collection about the purpose for collection, with whom information may be shared and for what purpose is recommended.<br>Provision of information about complaints mechanisms is supported. |

4.4

| APP 6 – use or disclosure of personal information |
|---|
| **The proposed principle is supported (in part - pending clarification)** |
| APP 6(1) and (2) are supported, in part.<br>APP 6(2)(g)(i) is not supported. This clause is extremely broad. Clear definition and procedure to test validity of an assumption that someone is 'missing' is required. There are many reasons an individual may decide to sever relationships or remove themselves. Inappropriate consideration of what constitutes 'missing' may pose a risk to an individual, for example, escaping a situation of family violence in that they may be reported by another as 'missing', but have chosen to flee. Any disclosure of their personal information may place them, and possibly others, at risk. This possible breach of privacy could extend to many areas of client contact and service provision.<br>APP 6(2)(h) is not supported without clarification of scope. Agencies and organisations are now required to provide information to the judiciary, where court orders apply, and for the purpose of other statutory obligations such as child protection investigations. There seems sufficient provision for disclosure throughout APP 6 and other legal obligations without the inclusion of this clause.<br>APP 6(3) is supported in principle. Guidance is required about what constitutes a 'written note' of disclosure, including the requirement for secure record keeping (refer Section 21: *Commissioner may make rules relating to certain matters*).<br>File notes of collection, use or disclosure of personal information should include:<br>• if consent was sought<br>• reasons for overriding the client's wishes or for not seeking consent<br>• advice disclosed, received or requested from others<br>• reasons for not agreeing to an information sharing request<br>• what information was collected, disclosed, with whom, and for what purpose<br>• any follow up activity required by the organisation or entity.<br>APP 6(5)(a) and (b) are supported. |

## 5 General comments

5.1 We strongly support a plain English approach to legislation to enable understanding and consistent application.

In their draft form, the Principles are difficult to interpret. Many small to medium-sized NGOs would be unable to allocate resources to develop organisational policies and procedures that translate the Principles into operational instruction. Similarly, training in its use will be either impeded or facilitated by the clarity of language and high order principles.

5.2 The draft legislation does not take a pro-disclosure approach to the sharing of information for protection of public safety and prevention of harm, abuse and neglect, that is, it is not encouraged or expected that information will be shared where serious harm is anticipated. Where APP 6 Subsection 2(c)(i)

applies it is recommended a pro-disclosure approach be considered for agencies and organisations that provide services to families and individuals.

Direct and indirect costs of failing to intervene early to support individuals and families at risk are substantial. Every family who is successfully supported to address vulnerabilities will offset costs to government from investigations, prosecutions, responding to homelessness and the provision of state care, mental health facilities, and drug and alcohol services. There is an opportunity to promote early intervention through improved information sharing between organisations and agencies where the disclosure promotes more effective service collaboration.

## 6 Conclusion

6.1 We welcome the proposal to have privacy principles that apply to public and private sectors and simplify obligations.

6.2 We support the adoption of a plain English approach to the APPs and any related companion guide or resources.

6.3 We fully support the intention to remove the test of imminence from the grounds for disclosure of personal information without consent where serious harm can be anticipated.

6.4 The benefit of sharing information to prevent serious harm could be strengthened by adopting a pro-disclosure approach to the application of APPs by relevant agencies and organisations.

6.5 The procedure adopted by government agencies and NGOs in South Australia to ensure that disclosure of personal information is secure, timely, accurate and relevant, and effectively balances the right to privacy and safety could be used as a template for guidance to other jurisdictions. That procedure is the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children Young People and their Families* (ISG).