Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2011

Executive Officer
Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 2343
ADELAIDE SA 5001
Phone (08) 8204 8786
privacy@sa.gov.au

September 2011

For information and advice, please contact:

The Presiding Member
Privacy Committee of South Australia
c/- State Records of South Australia
GPO Box 2343
ADELAIDE SA 5001

ph: (08) 8204 8786
fax: (08) 8204 8777
e-mail: privacy@sa.gov.au

This annual report has been issued pursuant to Clause 4A of the Proclamation of the Privacy Committee of South Australia.

The Hon Gail Gago MLC
MINISTER FOR PUBLIC SECTOR MANAGEMENT

Dear Minister

The Privacy Committee of South Australia is pleased to provide you with this report of its activities for the year ending 30 June 2011. The report is provided pursuant to Clause 4A of the *Proclamation establishing the Privacy Committee of South Australia*, as amended and republished in the South Australian Government Gazette on 11 June 2009.

Terry Ryan
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

30 September 2011

Table of Contents

1 Introduction

The administrative scheme for regulating the handling of personal information in the South Australian Government has been in place since 1989 and changed very little in that time. In contrast, society has changed significantly in the past twenty years, particularly in its technological development. The demands on Government have also changed with public expectation of more collaborative and efficient service delivery and greater access to government information. This increases the pressure on agencies to share personal information.

These developments place pressure on the framework aimed at protecting personal privacy. It is important that the public can remain confident in Government's ability to handle their personal information appropriately.

It is becoming evident through public comment and the media's response to a number of significant privacy breaches during the year that people are concerned about the protection of their personal information. The increasing mobility that new technology provides and the growing value of personal information adds to the threat of identity crime. In light of these challenges, the Privacy Committee continues to work with the Government to promote a high standard of information privacy protection in State Government as well as keeping itself informed of developments in other jurisdictions. Throughout the year, the Privacy Committee has provided advice, recommendations and support to numerous government agencies, undertaken research and contributed to national forums and consultations.

Notably, the Privacy Committee observed the further development of a number of national regulatory schemes, including those relating to childhood care, national heavy vehicle regulation and vocational education and training (VET). The Privacy Committee has endeavoured to ensure that it understands the privacy arrangements and potential impacts of these schemes and provided advice and recommendations where possible. The development of national laws for these schemes is quite complex due to the need to satisfy the differing requirements of all jurisdictions. During the year, the Privacy Committee specifically participated in consultation on the proposed national heavy vehicle laws and the national VET student identifier.

Further progress was achieved towards improving national consistency in Australian privacy law during the year. Significantly, the Australian Senate and Public Finance Administration Committee completed its review of the Exposure Draft Australian Privacy Principles (APPs). The APPs are seen as an important first step towards national consistency in privacy laws, providing a standard for privacy principles across Australia. It is important to note that the Senate Committee generally supported the draft APPs as an appropriate standard for the protection of personal information. However, it made twenty nine recommendations for improvement, including that the draft APPs be re-assessed to improve their clarity. The Privacy Committee looks forward to further progress in the reform of Australian privacy laws in 2011-12.

The Privacy Committee continued activities related to its role in granting exemptions from the IPPs, receiving privacy complaints and responding to

privacy enquiries. During the reporting year, the Privacy Committee granted eight exemptions from the IPPs to State Government agencies (see item 3.7), concluded five complaints (see item 3.6) and contributed to a number of consultation programs and inquiries (see items 3.2 and 3.3). The Executive Support to the Privacy Committee handled fewer enquiries from the public and State Government agencies compared to the previous year (see item 2.2.4).

This is a report of the activities of the Privacy Committee of South Australia (the Privacy Committee) for the year ending 30 June 2011. It has been developed pursuant to Clause 4A of the Proclamation establishing the Privacy Committee (see Appendix B).

2 South Australian Public Sector Privacy Framework

2.1 The Information Privacy Principles

South Australia's Information Privacy Principles (IPPs) were introduced in July 1989 by means of *Cabinet Administrative Instruction 1/89*, issued as *Premier & Cabinet Circular No. 12*, and more commonly known as the Information Privacy Principles Instruction.

The IPPs regulate the way South Australian Public Sector agencies collect, use, store and disclose personal information. A link to the Information Privacy Principles Instruction can be found on the State Records website at www.archives.sa.gov.au/privacy, and in Appendix A of this report.

2.2 The Privacy Committee of South Australia

2.2.1 Establishment and Functions

The Privacy Committee was established by Proclamation in the Government Gazette on 6 July 1989 and last varied on 11 June 2009. The functions of the Privacy Committee, as described in the Proclamation, are:

- to advise the Minister as to the need for, or desirability of, legislation or administrative action to protect individual privacy and for that purpose to keep itself informed as to developments in relation to the protection of individual privacy in other jurisdictions
- to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy
- to make publicly available information as to methods of protecting individual privacy and measures that can be taken to improve existing protection
- to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles are being implemented
- to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority
- such other functions as are determined by the Minister.

The scope of these functions is broader than the application of the IPPs and not necessarily restricted to activity within the South Australian Public Sector. However, the primary focus of the available resources (see item 2.2.4) is on matters that carry the greatest impact on the handling of personal information within State Government agencies bound by the IPPs.

A copy of the Proclamation can be found following the Information Privacy Principles Instruction, and in Appendix B of this report.

2.2.2 Reporting

During 2010-11, the Privacy Committee initially reported to the Hon Paul Holloway MLC, Minister Assisting the Premier in Cabinet Business and Public Sector Management and from 8 February 2011 to the Hon Gail Gago MLC, Minister for Public Sector Management.

2.2.3 Membership

There are six members of the Privacy Committee:

- three nominated by the Minister responsible (one of whom is not a public sector employee and one of whom will have expertise in information and records management)
- one nominated by the Attorney-General
- one nominated by the Minister for Health
- one nominated by the Commissioner for Public Employment.

This reporting year, the Privacy Committee comprised of:

Presiding Member:

- Terry Ryan, Director, State Records of South Australia, Department of the Premier and Cabinet

Members, in alphabetical order:

- Tanya Hosch, non-public sector employee
- Andrew Mills, Chief Information Officer, Government of South Australia
- Bernadette Quirke, Legal Counsel, Projects Branch, Department of Treasury and Finance, Crown Solicitor's Office
- Nancy Rogers, Manager, Research, Department for Families and Communities
- Andrew Stanley, Director, Policy, Legislation and Research, SA Health.

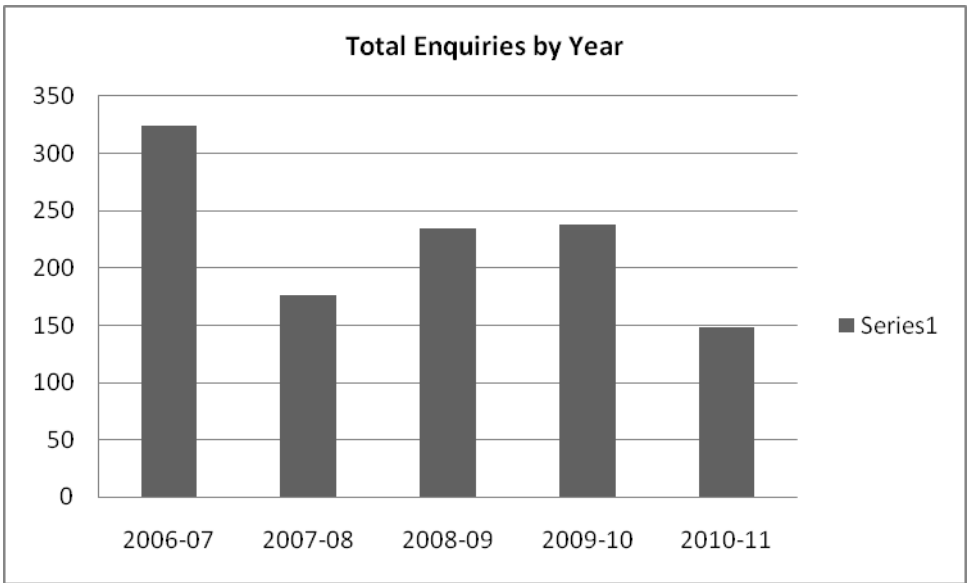
The term of appointment for each of the current members expires on 6 December 2012.

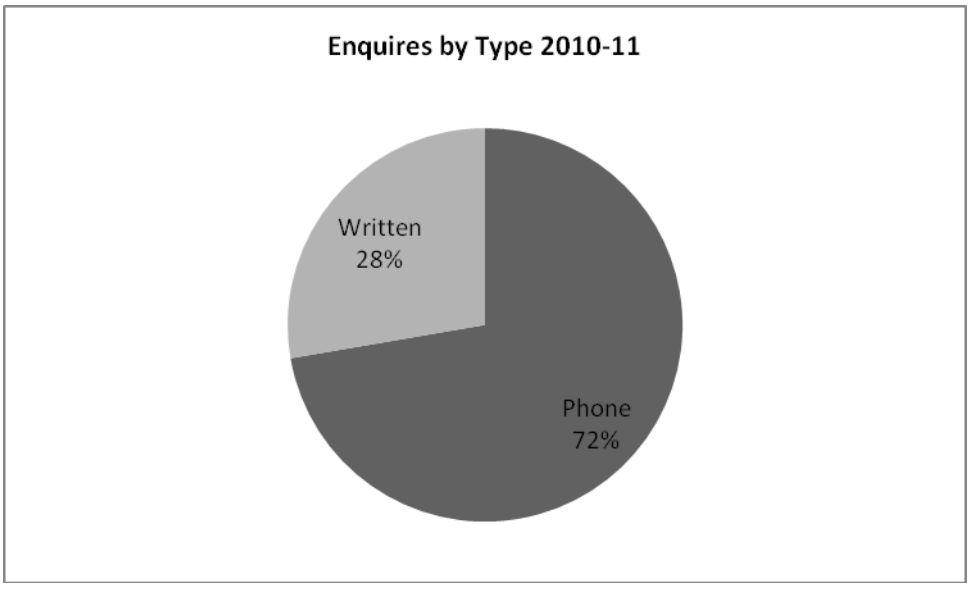
2.2.4 Resources

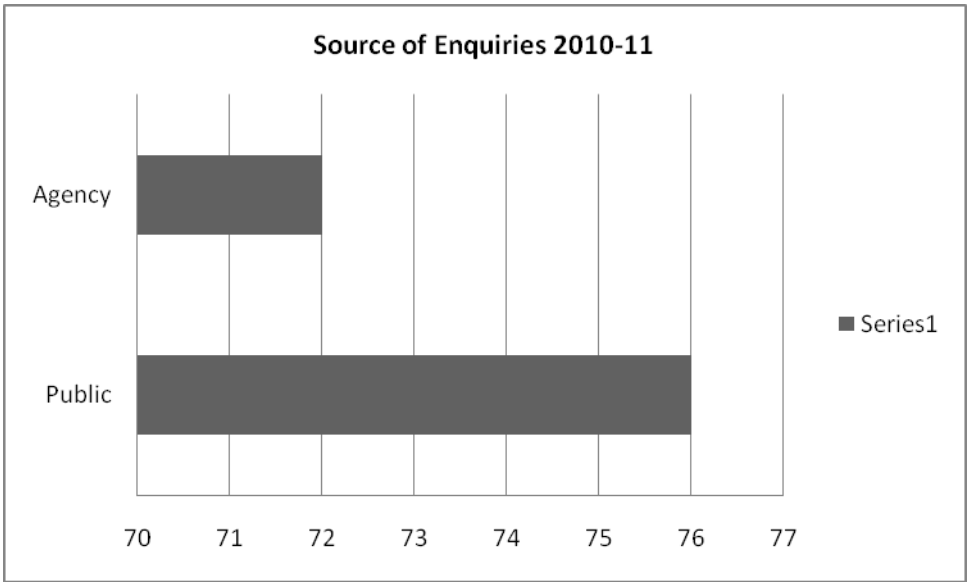
State Records of South Australia (State Records) provides support to the Privacy Committee including administrative support, meeting coordination, web hosting, an enquiry and advice service to both agencies and the public and a limited research function. This resource includes the commitment of approximately one full-time equivalent.

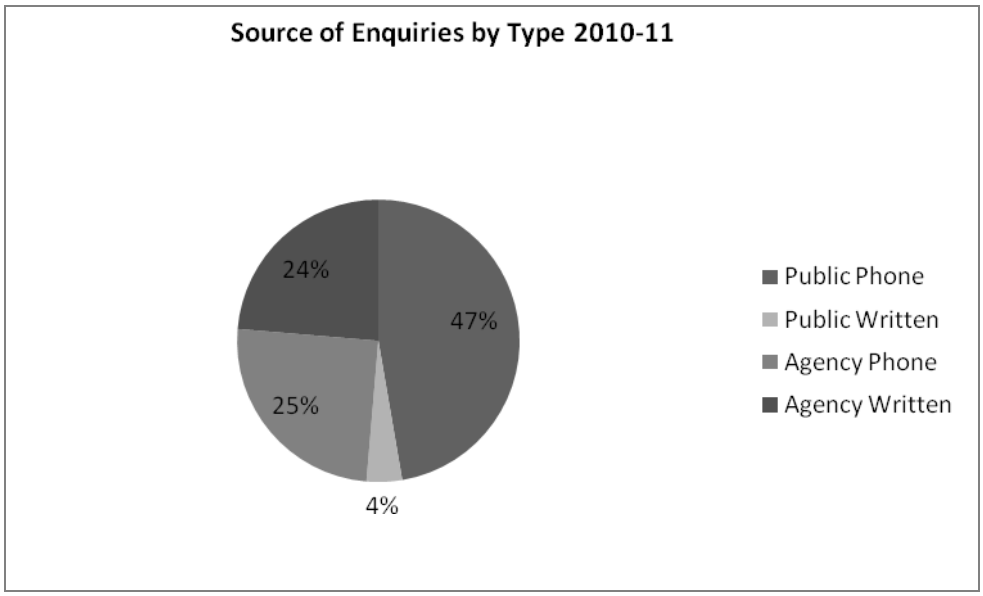
2.2.4.1 Privacy Enquiries

During the reporting year, State Records responded to 148 telephone and email enquiries from the public and State Government agencies relating to privacy of personal information. This represents a significant decrease in enquiries on the previous year, which may be explained partly by a reduction in the promotion of the Privacy Committee's contact information through local telephone directories. This was addressed in the later part of the year.









2.2.4.2 Privacy Training

Throughout the year, State Records conducted one Privacy Awareness training session for State Government employees. Privacy awareness is also included in the curriculum for the nationally accredited Certificate III in Business (Recordkeeping), which is developed and delivered by State Records.

2.2.5 Committee Remuneration

Premier & Cabinet Circular No. 16: Remuneration for Government Appointed Part-time Boards and Committees specifies the conditions under which members of Boards and Committees may be remunerated. In general, fees are not paid to Government employees, and so only the non-government member of the Privacy Committee is entitled to receive a sessional fee for meetings attended. The sessional fees are drawn from State Records' recurrent operating budget. More

information about the payment of fees can be found at *Premier & Cabinet Circular No. 16* available at www.premcab.sa.gov.au/pdf/circulars/Remuneration.pdf.

2.2.6 Meetings

During the reporting year the Privacy Committee met on 6 occasions. Meetings were supplemented by the conduct of business out of session.

2.2.7 Guidelines for members

A handbook for members contains information on the role of the Privacy Committee, its relationship to other approval and advisory bodies, duties and obligations of members, the process for handling complaints, and other information of value to members in performing their role. It also includes a brief history of privacy law and self-regulation in South Australia, and an overview of the protection of personal information in other Australian jurisdictions. The handbook also contains a Code of Conduct for members consistent with *Government Boards and Committees: Guidelines for Agencies and Board Directors* (Department of Premier and Cabinet, 2000).

A copy of the handbook can be found on the State Records website at www.archives.sa.gov.au/privacy/committee.html.

2.2.8 South Australia's Strategic Plan

South Australia's Strategic Plan 2007 (Strategic Plan) calls for performance improvement across the South Australian Public Sector in both government decision-making and administrative efficiency (Objective 1: Growing Prosperity: Targets T1.8 and T1.9). The Privacy Committee continues to improve in this area by implementing strategies such as the conduct of business out of session where appropriate to do so.

The constitution of the Privacy Committee meets Target T5.1 (Objective 5: Building Communities) to *'increase the number of women on all State Government boards and committees to 50% on average by 2008'*. During the reporting year the Privacy Committee maintained 50% female membership.

The activities of the Privacy Committee contribute to the achievement of other South Australia's Strategic Plan targets and priority actions across the South Australian Public Sector. Examples include:

- Objective 1: Growing Prosperity: Target T1.7: *'performance in the public sector – customer and client satisfaction with government services'* – the Australian public expects a high degree of privacy protection when accessing government services, and also expect a degree of control over how their personal information will be collected, stored, used and disclosed. There is also a high level of trust by the public that personal information held by State Government agencies is safe.
- Objective 2: Improving Wellbeing: there is a growing need for more holistic research and development in the areas of health, wellbeing and public safety. The use of personal information for research requires consideration of the IPPs to ensure the information is appropriately managed during and after completion of these activities.

3 Activities of the Privacy Committee

3.1 Advice to the Minister

The Privacy Committee has the function, under clause 2(a) of the Proclamation, *'to advise the Minister as to the need for, or desirability of, legislative or administrative action to protect individual privacy'*.

Throughout the reporting year, the Privacy Committee briefed the Minister on a range of matters relating to privacy. This included briefings related to national consistency in privacy law in Australia, privacy and e-health reform initiatives, Smartphone applications and the development of privacy legislation for South Australia. The Privacy Committee also provided advice to the Minister in relation to State Government initiatives that had the potential to impact on the privacy of individuals in South Australia.

3.2 Developments in other jurisdictions

The Privacy Committee has the function, under clause 2(a) of the Proclamation, *'to keep itself informed of developments in relation to the protection of individual privacy in other jurisdictions'*. Some key instances are described below.

3.2.1 Commonwealth, States and Territories

The Commonwealth and each State and Territory Government within Australia operate under varying legislative and administrative regimes for privacy protection. These regimes are of interest to the Privacy Committee as it considers its own responses to local and national issues. The following synopsis presents some of the more significant developments in other jurisdictions that have been noted by the Privacy Committee throughout the year.

3.2.1.1 Australian Privacy Law Reform

On 24 June 2010, the Australian Senate referred draft legislative amendments to the *Privacy Act 1988* to the Senate Finance and Public Administration Committee. The draft legislation follows from the Australian Government's response in October 2009 to the Australian Law Reform Committee's Review of Australian privacy law and practice. The first tranche of proposed amendments includes the replacement of the two existing sets of privacy principles in the Act with a single set of privacy principles, changes to credit reporting provisions, enhancing and clarifying health information arrangements and strengthening the Privacy Commissioner's powers.

The inquiry by the Senate Committee focussed on two issues during the year, exposure draft Australian Privacy Principles (APPs) and credit reporting provisions. The exposure draft APPs represent the Australian Government's first significant step towards improving national consistency in Australian privacy law. They will replace the two existing sets of privacy principles, the Information Privacy Principles, applying to the Commonwealth public sector and the National Privacy Principles, which apply to the private sector.

The draft APPs were subject to public consultation and a public hearing. The Senate Committee's final report was released on 15 June 2011. The Senate Committee reported that:

> *'the APPs contained in the exposure draft reflect the intent of the ALRC review and the needs of the Government to ensure that standards are in place to address the risk of harm from the inappropriate collection, use and disclosure of personal information and to meet the expectations of individuals that personal information will be handled appropriately.'*

However, the Senate Committee made twenty nine recommendations for improvement to the draft APPs including those aimed at:

- Improving their simplicity and clarity;
- Removing agency specific exceptions; and
- Improving guidance on concepts and terms used in the principles.

The Privacy Committee provided advice to the Minister and Government on the draft APPs, particularly in light of the Commonwealth's commitment to national consistency in privacy laws. The Privacy Committee looks forward to further progress on this reform in 2011-12.

3.2.1.3 National Electronic Health Reform

Building on the foundations laid by the introduction of the National Healthcare Identifier Service in July 2010, the Australian Government continued to progress toward the introduction of a national system for electronic health records by July 2012. The aim of the proposed system is to give all Australians the option to sign up for a Personally Controlled Electronic Health Record (PCEHR). The system is aimed at providing individuals the opportunity to see their health information when and where they need it and share this information with relevant healthcare providers. Healthcare providers see it as a potential for better decision making.

The Privacy Committee has kept itself informed of developments in the PCEHR system throughout the year and noted specifically the release of the Draft Concept of Operations in April 2011. The protection of individual privacy of the personal information within the PCEHR system is essential to its success. The Privacy Committee will continue to keep itself informed of this project as it progresses in 2011-12.

3.2.1.4 National Heavy Vehicle Regulation

The Privacy Committee was consulted on the development of the proposed National Heavy Vehicle Laws during the year.

The proposed national law is being developed with the aim of reducing red tape and improving productivity and safety in the heavy vehicle industry. The proposed law will be administered by the new National Heavy Vehicle Regulator, expected to be operational by 1 January 2013 and will apply to all vehicles over 4.5 tonnes.

The Exposure Draft National Heavy Vehicle laws were released for public consultation on 28 February 2011. The Privacy Committee provided advice to the Department of Transport, Energy and Infrastructure on the information

privacy arrangements under the proposed laws to support the State's response to national consultations.

3.2.1.5 Other Commonwealth and National initiatives

During the year, the Privacy Committee participated in consultation on the proposed introduction of a National Vocational Education and Training (VET) Student Identifier and kept itself informed of the development of the National Education and Care Services Legislation.

On 7 December 2009, the Council of Australian Government's approved in-principle the introduction of a National VET Student Identifier from 2012. The aims of the identifier is to track students as they progress through their education and training, to support the collection of better data on the VET system and to improve student's capacity to manage their learning and skills development. The National Centre for Vocational Education Research was charged with responsibility for developing a business case for the implementation of the identifier and undertook consultation on the proposed student identifier in May 2011. The Privacy Committee participated in a consultation interview as part of this process.

During the year, the Privacy Committee also kept itself informed of the development of the privacy arrangements under the Education and Care Services National Law and associated regulations. The law is to establish the National Quality Framework for Early Childhood Education and Care, to come into effect from 1 January 2012. The laws will set a new National Quality Standard and regulatory framework for long day care, family day care, preschool and outside school hours care services in all States and Territories.

Understanding the risks and benefits of the varied approaches for managing information privacy under national regulatory schemes has been a challenge for privacy authorities across Australia. . The Privacy Committee is committed to working with the Government and other Australian privacy authorities to promote the maintenance of information privacy protections in national regulatory schemes.

3.2.2 Meetings and seminars

Throughout the year, representation of the Privacy Committee at various meetings, seminars and forums, included attendance at:

- one meeting of the Asia Pacific Privacy Authorities (APPA);
- two meetings of the Privacy Authorities of Australia (PAA); and
- the Right to Information Day Forum in Brisbane in September 2009.

The Privacy Committee participated in the South Australian Law Society's 'Privacy Law Update', as part of the Society's compulsory professional development program. The Committee also provided a privacy awareness presentation for a forum organised by the South Australia chapter of the Records and Information Management Professionals Australasia in October 2010.

3.2.2.1 Asia Pacific Privacy Authorities (APPA)

APPA convenes twice a year with meetings hosted on a rotating basis by the various member authorities. At the meetings, issues are discussed such as privacy and security, identity management, surveillance, cross-jurisdictional law enforcement between countries in the Pacific Rim, privacy legislation amendments, cryptography and personal data privacy. The Privacy Committee has observer status at APPA as it is not considered an independent statutory privacy or data protection authority.

The Privacy Committee was represented at the meeting of APPA held in Auckland on 7 to 8 December 2010. The meeting considered issues including:

- Direct marketing and privacy
- Implications of Web 2.0 technologies on privacy regulation
- International privacy developments.

Further information about APPA can be found on the Australian Privacy Commissioner's website at
http://www.privacy.gov.au/international/appa/index.html

3.2.2.2 Privacy Authorities of Australia (PAA)

The Privacy Committee was represented at two meetings of the PAA on 20 September 2010 and 11 March 2011.

PAA membership consists of representation of privacy authorities from Australian jurisdictions that meet informally to encourage knowledge sharing and cooperation on privacy issues specific to Australia. The group was first formed in 2008 and provides the Committee with an opportunity to connect with other Australian privacy authorities and stay informed about developments in their jurisdictions.

The PAA terms of reference include:

- facilitating the sharing of knowledge and resources between privacy agencies and authorities within Australia
- fostering cooperation in privacy and data protection
- promoting best practice and consistency amongst privacy agencies and authorities
- working to continuously improve our performance to achieve the important objectives set out in our respective privacy laws or policies.

The Privacy Committee was represented at two meetings of the PAA in 2010-11. The September 2010 meeting was hosted by Privacy Victoria and considered privacy issues in relation to:

- national regulatory schemes
- cooperation between PAA members
- memorandums of understanding between government agencies and private sector organisations.

The Privacy Committee hosted the PAA meeting of 11 March 2011 in Adelaide. The meeting addressed a number of issues across Australian jurisdictions, including:

- privacy arrangements in National Regulatory Schemes;
- information sharing in the child protection context;.
- data linkage for research and privacy; and
- cooperation between PAA member authorities.

3.3 Recommendations and submissions

The Privacy Committee has the function, under clause 2(b) of the Proclamation, *'to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy'*.

The Privacy Committee responded to various requests for advice, support and recommendations. Key instances are described below.

3.3.1 Implementation of Amendments to the Information Privacy Principles (IPPs)

On 18 May 2009, the Government approved amendments to the IPPs to recognise the activity of businesses performing services on behalf of government. These amendments addressed the gap that existed in the application of privacy principles to service providers contracted to the South Australian Government.

The work undertaken to progress the implementation of the amendments during the year included improving the Committee's guidance on contracting and the IPPs and writing to agency Chief Executives to remind them of the amendments. The Privacy Committee also provided advice to a number of agencies on issues associated with contracted service provision and compliance with the IPPs.

3.3.2 SA NT DataLink

SA NT DataLink is the operational body of a joint venture consortium of South Australian and Northern Territory Government agencies and non-government organisations and universities. SA NT DataLink is responsible for the development, maintenance and operation of a Data Linkage System (the System) that allows health, social and economic research, education and policy development to be undertaken with de-identified data in South Australia and the Northern Territory. The System is aimed at providing an improved evidence base for research, while minimising risks to individual privacy when compared to traditional sample based research methods.

The SA NT data linkage project continued to progress during 2010-11, with a number of new data sets being added to the System to support current demonstration projects, including the:

- Colorectal cancer project; and
- SA early childhood development project.

During 2010-11, the Privacy Committee continued to work with SA NT DataLink on the privacy and governance arrangements for the System. In addition, the Privacy Committee provided four exemptions from the IPPs to facilitate the

further establishment of the System. These exemptions were provided where the Privacy Committee deemed them to be in the public interest.

Further information on SA NT DataLink and current research projects can be found at www.santdatalink.org.au

(See Appendix H for the full text of the exemptions provided in relation to SA NT DataLink)

3.3.4 Identity Security and Information Privacy

Identity security management has strong links with information privacy protection with one of the major risks of identity related crimes involving the theft or misuse of an individual's personal information. State Government agencies hold information critical to an individual's proof of identity, such as birth and marriage records and government issued licences. The Privacy Committee continued to provide advice to agencies on the protection of personal information to support identity security management during the reporting year. The Committee specifically provided advice on the Department of Transport, Energy and Infrastructure's evidence of identity policy and participated in State consultations with the Commonwealth on the National Identity Security Strategy.

3.3.5 Online Applications and the IPPs

One of the major technological developments with potential to impact on information privacy in recent years is in online software applications, specifically those developed for mobile computing platforms, such as Smartphones and tablet computers[1]. During the year, the Privacy Committee kept itself informed of developments across the world in this area and their potential to impact on information privacy in South Australia. The Committee also commenced a review of the development of applications for mobile devices by Government agencies. The review is expected to be completed in early 2011-12.

3.3.6 National Government Information Sharing Strategy

The National Government Information Sharing Strategy (NGISS) was endorsed by the Council of Australian Government's (COAG) Online and Communication Council (OCC) in December 2008. The NGISS is to provide a standardised approach to information sharing to support the delivery of government services to the Australian community. The expectation is that the national strategy can be used at all levels of government. A key principle promoted by the NGISS is ensuring privacy and security in the sharing of government information.

During the year, the Privacy Committee provided advice to the Office of the Chief Information Officer to support work being undertaken in the implementation of the NGISS in South Australian Government agencies.

[1] A Smartphone is a mobile phone with advanced computing functionality. A tablet computer is a single screen highly portable personal computer.

3.4 Communication

The Privacy Committee has the function, under clause 2(c) of the Proclamation, *'to make publicly available, information as to methods of protecting individual privacy and measures that can be taken to improve existing protection'*.

3.4.1 Privacy Officer Network

The Privacy Officer Network (the Network) was established in September 2006 to assist Principal Officers of agencies fulfill their obligation to comply with the IPPs, and to increase the efficiency of communications about the handling of personal information held by State Government agencies. State Records coordinates and provides support to the Network. The aim of the Network is to contribute to the improvement of privacy awareness across the public sector.

No formal meetings of the Privacy Officer Network were held during 2011-12.

3.4.2 Participation in committees and groups

When the opportunity arises, the Privacy Committee is represented at meetings with Commonwealth, State and Territory Governments as deemed appropriate.

The Privacy Committee is represented on the APPA (see also item 3.2.3.1) and PAA (see also item 3.2.3.2).

The Presiding Member is also a member of the South Australian Government's ICT Security and Risk Steering Committee.

3.5 Keep informed as to the extent to which the Information Privacy Principles are implemented

The Privacy Committee has the function, under clause 2(d) of the Proclamation, *'to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles are being implemented'*.

The Privacy Committee seeks reports from agencies from time to time. See section 3.3.

3.6 Complaints

The Privacy Committee has the function, under clause 2(g) of the Proclamation, *'to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority'*.

In the first instance, the Privacy Committee will generally forward complaints it has received to the agency concerned and seek a response as to whether they consider a breach of the Information Privacy Principles has occurred and, if so, what action has been or might be taken to resolve the matter. The Privacy Committee will assess the response and, if necessary, make a recommendation to the agency to amend their practices or to adopt other measures to resolve the complaint. The Privacy Committee may also refer the complainant to the South Australian Ombudsman if they remain dissatisfied with the agency's response.

If the complaint relates to privacy breaches in the delivery of Government health services, the Committee may refer the complaint to the Health and Community Services Complaints Commissioner. If the complaint relates to privacy breaches in relation to the South Australian Police, the Committee may refer the complaint to the Police Complaints Authority.

The Committee will also accept privacy complaints in relation to South Australian Universities and Local Government. While there is no legislated or administrative privacy regime that applies to these organisations, the Committee has previously worked with both these sectors of government to resolve privacy complaints and improve their practices when handling personal information.

During the reporting year there were two new formal complaints received and four pre-existing complaints that underwent further deliberation. Of the six complaints handled, five were concluded and one is still to be finalised. A summary of the complaints concluded during the year is outlined in the table below.

3.6.1 Complaints Concluded Summary Table

	Respondent Organisation	**Information Privacy Principle (IPP)**	**Other Privacy Issue**	**Outcome**
1	Government Dept	IPP10		No breach - disclosure required or authorised by law
2	Government Dept	IPP10		No breach - disclosure required or authorised by law
3	Local Government Council		Video Surveillance	CCTV Camera removed
4	Government Dept	IPP 10		No breach – disclosure required or authorised by law
5	Independent Judicial Body	n/a	Disclosure of personal information	The Independent Judicial Body was not an agency for the purposes of the IPPI

3.6.2 Local Government complaints

The Privacy Committee concluded one privacy complaint concerning a Local Government Authority during 2010-11. The complaint concerned video surveillance by a Council. As a result of the complaint, the Council agreed to cease the video surveillance.

3.7 Exemptions

The Privacy Committee may, under clause 4 of the Proclamation, *'exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Privacy Committee thinks fit'*.

Requests for exemptions are considered on a case-by-case basis. Exemptions are only applied in situations where the public interest for an activity outweighs the privacy protections afforded by the IPPs, or where otherwise warranted by unique circumstances. Exemptions are generally subject to conditions including an expiry date and a requirement for agencies to report on the activity conducted under the exemption.

During the reporting year, eight individual exemptions were approved. Of the eight exemptions, three related directly to specific research projects. It is important to note that the IPPI does not provide for the disclosure of personal information without consent for research purposes. Following is a summary of each of the requests for exemption.

3.7.1 SA NT DataLink

The Privacy Committee dealt with four submissions from SA NT DataLink during the year seeking exemptions from the IPPs. The exemptions were sought in line with the governance arrangements established between the Privacy Committee and SA NT DataLink to facilitate the development of the Data Linkage System.

The Privacy Committee granted exemptions allowing the disclosure of limited personal information from government datasets to officers of SA Health located within SA NT DataLink, the information was to be used only for the establishment of the master linkage file in the Data Linkage System. The exemptions related to the following government datasets:

- South Australian Dental Service dataset
- Child, Womens' and Youth Health dataset
- South Australian Perinatal dataset
- South Australian Births and Deaths datasets.

See 3.3.2 for more information on the SA Data Linkage Project and Appendix C for the full text of the exemptions.

3.7.2 Housing SA and SAPOL Ministerial Agreement

In October 2010, the Privacy Committee received a joint submission from the South Australia Police (SAPOL) and Housing SA seeking exemption from IPPs 8 and 10 to permit use and disclosure of personal information under a Ministerial Agreement promoting cooperation between the agencies to address social disorder and criminal activity in South Australian Housing Trust properties.

In November 2010, the Privacy Committee granted the exemption to permit the exchange of personal information between the agencies where it was reasonably necessary to prevent damage to property, disorderly or violent conduct (towards a person or property) or conduct that would otherwise disturb the public peace.

See Appendix D for the full text of the exemption.

3.7.3 Offender Management Plan

In February 2010, the Privacy Committee received a joint submission from South Australia Police, the Department for Correctional Services, the Department for Families and Communities and the Department of Health for an exemption from IPPs 2, 8 and 10 to allow for information sharing between the agencies through a pilot program of the South Australia Offender Management Plan (the Plan). The exemption was provided for up to 12 months or until the completion of the pilot program, whichever was earlier. In February 2011, the Committee received a further submission seeking to extend the exemption for a further twelve months, to support an extension of the pilot program. The Committee

granted a further twelve month exemption to permit information sharing under the pilot program.

The purpose of the Plan is to provide coordinated case management of serious adult offenders who present the most harm to the community in order to improve rehabilitation outcomes and promote community safety.

The exemption is restricted to information relevant to the coordinated case management of the selected offenders under the pilot program and conditional on those offenders being informed of their inclusion in the pilot program.

See Appendix E for the full text of the exemptions.

3.7.4 Offender Management Plan – OCSAR Evaluation

On 28 June 2010, the Privacy Committee received a submission from the Office of Crime Statistics and Research (OCSAR) seeking an exemption from the IPPs to allow it to undertake an evaluation of the pilot program of the Offender Management Plan.

At its meeting on 16 July 2010, the Privacy Committee approved an exemption from IPPs 2 and 8 for 12 months to permit the collection and use of personal information in OCSAR's evaluation of the pilot program. The exemption was conditional on OCSAR operating in accordance with the Offender Management Plan Information Sharing Protocol and that offenders participating in the pilot program were informed of the evaluation.

See Appendix F for the full text of the exemption.

3.7.5 Community Protection Panel – OCSAR Evaluation

In September 2010 the Committee received a submission from OCSAR seeking an exemption from IPPs 2 and 8 permitting it to collect and use personal information as part of its evaluation of the Community Protection Panel (CCP). The role of the CPP is to enable a multi-agency approach to the management of serious repeat young offenders.

The Privacy Committee granted the exemption on 8 October 2010. The exemption was conditional on OCSAR obtaining approval for the evaluation from the Department for Families and Communities Human Research Ethics Committee and the Aboriginal Health Research and Ethics Committee. It was also conditional on OCSAR ensuring that the outcome of the evaluation would not result in the disclosure of personal information to a third party in a form that would identify an individual offender or from which an individual offender would be reasonably identifiable.

See Appendix G for the full text of the exemption

3.7.6 Early Intervention Pilot Program – OCSAR Evaluation

On 8 July 2010, the Privacy Committee received a submission from OCSAR seeking an amendment to the exemption from the IPPs granted by the Committee in relation to OCSAR's evaluation of the Early Intervention Pilot Program (EIPP). The EIPP allows South Australia's police, courts and health services to work in partnership to help young people at risk of abusing alcohol.

The proposed amendment to the exemption was to include the collection of personal information from the Family Conference Team in the Courts Administration Authority for the purposes of the OCSAR evaluation.

The Privacy Committee amended the exemption on 26 August 2010.

See Appendix H for the full text of the exemption.

3.7.7 Information Sharing Guidelines

On 6 April 2011, the Privacy Committee considered and approved the extension of the exemption from IPP 10(b) granted to agencies utilising the *Information Sharing Guidelines for Promoting the Protection of Children, Young People and their Families* (ISG). The ISG was introduced in 2008 and provides a clear framework for sharing information to support early intervention in the protection of children and young people.

The exemption is conditional on the Office of the Guardian reporting to the Privacy Committee on the progress of implementation after 12 months. The exemption is also to be reviewed by the Office of the Guardian and the Privacy Committee two years after its approval.

See Appendix I for the full text of the exemption.

Appendices

A Information Privacy Principles

Cabinet Administrative Instruction 1/89, also known as the Information Privacy Principles (IPPs) Instruction, and premier and cabinet circular 12, AS AMENDED BY CABINET 18 May 2009

Government of South Australia

Cabinet Administrative Instruction No.1 of 1989

(Re-issued 30 July 1992 and 18 May 2009)

PART 1
PRELIMINARY

Short Title

1. This Instruction may be called the "Information Privacy Principles Instruction".

Commencement and Application

2. (1) This Instruction will come into effect on 18 May 2009.

(2) Subject to any contrary determination by Cabinet, this Instruction shall apply to "the public sector agencies" as that expression is defined in Section 3(1) of the *Public Sector Management Act 1995.*

(3) This Instruction shall not apply to an agency that appears in the attached schedule.

Interpretation

3. (1) In this Instruction-

"agency" means a public sector agency that falls within the scope of application of this Instruction pursuant to the provisions of Clause 2(2).

"the Committee" means the Privacy Committee of South Australia constituted by Proclamation.

“contracted service provider” means a third party that enters into a contract with an agency to provide goods or services required by an agency for its operations.

“contract for service” means that contract between the contracted service provider and the agency.

"personal information" means information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person

whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

"principal officer" means in relation to an agency:

(a) the person holding, or performing duties of, the Office of Chief Executive Officer of the agency;

(b) if the Commissioner for Public Employment declares an office to be the principal office in respect of the agency - the person holding, or performing the duties of, that office; or

(c) in any other case - the person who constitutes that agency or, if the agency is constituted by two or more persons, the person who is entitled to preside at any meeting of the agency at which the person is present.

"the Principles" means the Information Privacy Principles established under Clause 4 of this Instruction.

"record-subject" means a person to whom personal information relates.

(2) A reference to any legislation, regulation or statutory instrument in this Instruction shall be deemed to include any amendment, repeal or substitution thereof.

(3) A reference to a person, including a body corporate, in this Instruction shall be deemed to include that person's successors.

PART II
INFORMATION PRIVACY PRINCIPLES

Principles

4. The principal officer of each agency shall ensure that the following Principles are implemented, maintained and observed for and in respect of all personal information for which his or her agency is responsible.

Collection of Personal Information

(1) Personal information should be not collected by unlawful or unfair means, nor should it be collected unnecessarily.

(2) An agency that collects personal information should take reasonable steps to ensure that, before it collects it or, if that is not practicable, as soon as practicable after it collects it, the record-subject is told:

(a) the purpose for which the information is being collected (the "purpose of collection"), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law - that the collection of the information is so authorised or required; and

(c) in general terms, of its usual practices with respect to disclosure of personal information of the kind collected.

(3) An agency should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out of date, incomplete or excessively personal.

Storage of Personal Information

(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.

Access to Records of Personal Information

(5) Where an agency has in its possession or under its control records of personal information, the record-subject should be entitled to have access to those records in accordance with the *Freedom of Information Act 1991*.

Correction of Personal Information

(6) An agency that has in its possession or under its control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, incomplete, irrelevant, out of date, or where it would give a misleading impression in accordance with the *Freedom of Information Act 1991*.

Use of Personal Information

(7) Personal information should not be used except for a purpose to which it is relevant.

(8) Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless:

(a) the record-subject has expressly or impliedly consented to the use;

(b) the agency using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person;

(c) the use is required by or under law; or

(d) the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

(9) An agency that uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of Personal Information

(10) An agency should not disclose personal information about some other person to a third person unless:

(a) the record-subject has expressly or impliedly consented to the disclosure;

(b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person;

(c) the disclosure is required or authorised by or under law; or

(d) the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

Acts and Practices of Agency and Contracted Service Provider

5. For the purposes of this Instruction-

(a) an act done or practice engaged in by, or personal information disclosed to, a person employed by, or in the service of, an agency in the performance of the duties of the person's employment shall be deemed to have been done or engaged in by, or disclosed to, the agency;

(b) an act done or practice engaged in by, or personal information disclosed to, a person on behalf of, or for the purposes of the activities of, an unincorporated body, being a board, council, committee, subcommittee or other body established by, or in accordance with, an enactment for the purpose of assisting, or performing functions in connection with, an agency, shall be deemed to have been done or engaged in by, or disclosed to, the agency.

(c) subject to clause 5(A), an act done or a practice engaged in by, or personal information disclosed to, a person employed by, or in the service of, a person or organisation providing services to an agency under a contract for services for the purpose of or in the course of performance of that contract shall be deemed to have been done or engaged in by, or disclosed to, the agency.

5(A) A contract for service, which will necessitate the disclosure of personal information to a contracted service provider, must include conditions to ensure that these Principles are complied with as if the Contracted Service Provider were part of the agency and must include provisions that enable audit and verification of compliance with these obligations.

Agencies to comply with Principles

6. An agency shall not do an act or engage in a practice that is in breach of or is a contravention of the Principles.

Collecting of Personal Information

7. For the purposes of the Principles, personal information shall be taken to be collected by an agency from a person if the person provides that information to the agency in response to a request by the agency for that information or for a kind of information in which that information is included.

PART III
COMPLIANCE WITH PRINCIPLES

8. The Committee may at any time on its own initiative appoint a person (whether or not that person is a public employee) or the Commissioner for Public Employment to investigate or assist in the investigation of the nature and extent of compliance of an agency with the Principles and to furnish a report to the Committee accordingly.

Reporting Procedures Pursuant to this Instruction

9. Each principal officer shall furnish to the Committee such information as the Committee requires and shall comply with any requirements determined by the Committee concerning the furnishings of that information including:

   (a) the action taken to ensure that the Principles are implemented, maintained and observed in the agency for which he or she is responsible;

   (b) the name and designation of each officer with authority to ensure that the Principles are so implemented, maintained and observed;

   (c) the result of any investigation and report, under Clause 8, in relation to the agency for which he or she is responsible and, where applicable, any remedial action taken or proposed to be taken in consequence.

Agencies Acting Singly or in Combination

10. This Instruction and the Principles shall apply to the collection, storage, access to records, correction, use and disclosure in respect of personal information whether that personal information is contained in a record in the sole possession or under the sole control of an agency or is contained in a record in the joint or under the joint control of any number of agencies.

SCHEDULE: CLAUSE 2 (3)
AGENCIES TO WHICH THIS INSTRUCTION DOES NOT APPLY

South Australian Asset Management Corporation

Motor Accident Commission (formerly State Government Insurance Commission)

WorkCover Corporation of South Australia

B Proclamation of the Privacy Committee of South Australia

Version: 11.6.2009

South Australia

Privacy Committee of South Australia

1—Establishment and procedures of Privacy Committee of South Australia

(1) My Government will establish a committee to be known as the *Privacy Committee of South Australia*.

(2) The Committee will consist of six members appointed by the Minister as follows:

(a) three will be chosen by the Minister, and of these one must be a person who is not a public sector employee (within the meaning of the *Public Sector Management Act 1995* as amended or substituted from time to time) and one must be a person with expertise in information and records management;

(b) one will be appointed on the nomination of the Attorney-General;

(c) one will be appointed on the nomination of the Minister responsible for the administration of the *Health Care Act 2008* (as amended or substituted from time to time); and

(d) one will be appointed on the nomination of the Commissioner for Public Employment (and, for the purposes of this paragraph, the reference to the Commissioner will, if the title of the Commissioner is altered, be read as a reference to the Commissioner under his or her new title).

(2aa) At least 2 members of the Committee must be women and at least 2 must be men.

(2a) One of the persons appointed under subclause (2)(a) will be appointed (on the nomination of the Minister) to be the presiding member.

(3) A member will be appointed for a term not exceeding four years.

(3a) Where a member is appointed for a term of less than four years, the Minister may, with the consent of the member, extend the term of the appointment for a period ending on or before the fourth anniversary of the day on which the appointment took effect.

(4) The office of a member becomes vacant if the member—

(a) dies;

(b) completes a term of office and is not reappointed;

(c) resigns by written notice to the Minister; or

(d) is removed from office by the Governor on the ground of—

(i) mental or physical incapacity to carry out official duties satisfactorily;

(ii) neglect of duty;

(iii) disclosure of information by the member contrary to clause 3(2); or

(iv) misconduct.

(5) Subject to the following, the Committee may determine its own procedures:

(a) a meeting of the Committee will be chaired by the presiding member or, in his or her absence, by a member chosen by those present;

(b) subject to paragraph (c), the Committee may act notwithstanding vacancies in its membership;

(c) four members constitute a quorum for a meeting of the Committee;

(d) a decision in which a majority of the members present at a meeting concur is a decision of the Committee but if the members are equally divided the person presiding at the meeting will have a casting vote;

(e) a member who is unable to attend a meeting of the Committee may, with the approval of the presiding member, be represented for voting and all other purposes at the meeting by his or her nominee;

(g) the Committee must keep minutes of its proceedings.

(6) In performing its functions the Committee may consult any person and may establish subcommittees of at least two of its members to assist and advise it.

2—Functions of the Committee

The Committee will have the following functions:

(a) to advise the Minister as to the need for, or desirability of, legislation or administrative action to protect individual privacy and for that purpose to keep itself informed as to developments in relation to the protection of individual privacy in other jurisdictions;

(b) to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy;

(c) to make publicly available information as to methods of protecting individual privacy and measures that can be taken to improve existing protection;

(d) to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles are being implemented;

(g) to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority;

(h) such other functions as are determined by the Minister.

3—Prohibition against disclosure of information

(2) A member of the Committee must not disclose any information acquired by the member by virtue of his or her membership of the Committee except—

(a) in the course of performing duties and functions as a member of the Committee; or

(b) as required or authorized by law.

4—Exemptions

(1) The Committee may exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit.

4A—Annual report

(1) The Committee must, on or before 30 September in each year, prepare and present to the Minister a report on its activities during the preceding financial year.

(2) The report must include details of any exemptions granted under clause 4 during the year to which the report relates.

(3) The Minister must, within 12 sitting days after receipt of a report under this section, cause copies of the report to be laid before each House of Parliament.

5—Interpretation

In this proclamation, unless the contrary intention appears—

Information Privacy Principles means the principles set out in Part II of Cabinet Administrative Instruction No. 1 of 1989 entitled "Information Privacy Principles Instruction"

Minister means the Minister who is, for the time being, responsible for the Committee.

C Exemptions Granted – SA NT DataLink

Exemption - South Australian Dental (Titanium) Dataset

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[2] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department of Health (DH). It is an exemption from compliance with Principle 8 and 10, allowing DH to use personal information for a purpose that was not the purpose of the collection of that information and to disclose that information to South Australian Northern Territory DataLink (SA NT DataLink).

The personal information to be used is from DH's South Australian Dental (Titanium) Dataset and is limited to:

- Unique record identifier
- Unique personal identifier where available
- Names (all including "aka's" aliases and nicknames
- Data of birth
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Country of birth
- Full address including geocodes where available
- Any of the above information provided for other family members and included in these records.

The information is to be used for the creation of master linkage keys as part of the establishment of the Data Linkage System by officers of DH within SA NT DataLink.

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the establishment of the Master Linkage File as part of the Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of DH.

DH remains responsible for the secure transfer and storage of personal information in line with the Information Privacy Principles.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

---

[2] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

Expiry

This exemption will be reviewed by DH and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

19 July 2010

Exemption - Child, Youth and Women's Health Service dataset

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[3] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department of Health (SA Health). It is an exemption from compliance with Principles 8 and 10, allowing SA Health to use personal information for a purpose that was not the purpose of the collection of that information and to disclose that information to South Australian Northern Territory DataLink (SA NT DataLink).

The personal information to be used is from Child, Youth and Women's Health Service dataset and is limited to:

- Unique Record Identifier
- Unique Person Identifier where available
- Names
- Date of Birth
- Birth Weight
- Sex
- Title
- Aboriginality, Torres Strait Islander Indicator
- Country of birth
- Full address including geocodes if available
- Any of the above information provided for other family members and included in these records.

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the establishment of the Master Linkage File as part of the Data Linkage System by

[3] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

officers of SA Health within SA NT DataLink. The exemption is provided on the condition that the personal information is only to be accessed by officers of SA Health.

SA Health remains responsible for the secure transfer and storage of personal information in line with the IPPs.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption will be reviewed by SA Health and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

23 December 2010

Exemption - South Australian Perinatal dataset

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[4] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department of Health (SA Health). It is an exemption from compliance with Principles 8 and 10, allowing SA Health to use personal information for a purpose that was not the purpose of the collection of that information and to disclose that information to South Australian Northern Territory DataLink (SA NT DataLink).

The personal information to be used and disclosed is from the South Australian Perinatal dataset and is limited to:

Mother and baby variables

- Unique record identifier
- Unique person identifier where available
- Names – all names including nicknames, aliases and aka
- Date of birth
- Sex
- Title
- Aboriginality, Torres Strait Islander Indicator

[4] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

- Country of birth
- Full address including geocodes if available.

Additional variables

- Baby's birth weight
- Plurality – order and total
- Mother's occupation
- Father's occupation.

The use and disclosure will include any of the above information provided for other family members that is included in these records.

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the establishment of the Master Linkage File as part of the Data Linkage System by officers of SA Health within SA NT DataLink. The exemption is provided on the condition that the personal information is only to be accessed by officers of SA Health.

SA Health remains responsible for the secure transfer and storage of personal information in line with the IPPs.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption will be reviewed by SA Health and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

1 February 2011

Exemption - South Australian births and deaths datasets

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[5] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

[5] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

This exemption applies to the Department of Health (SA Health). It is an exemption from compliance with Principle 8, allowing SA Health to use personal information for a purpose that was not the purpose of the collection of that information. The personal information is to be used in the establishment of the Master Linkage File as part of the Data Linkage System.

The personal information to be used is from the South Australian births and deaths datasets and is limited to:

Death Dataset

- Unique record identifier (registration number)
- Names (all names where available including surnames, surnames at birth, given names and given names at birth)
- Date of birth
- Date of death
- Age at death
- Place of birth
- Place of death
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Full residential address, including geocodes, where available.

Birth Dataset

The following personal information to be used from the births dataset is limited to birth records within the data range 1/1/1999 to 31/12/2005.

- Unique record identifier (registration number)
- Names (all names where available including surnames, surnames at birth, given names and given names at birth)
- Full residential address, including geocodes where available
- Sex
- Date of birth
- Place of birth
- Mother's Aboriginal indicator
- Mother's Torres Strait Islander indicator
- Father's Aboriginal indicator
- Father's Torres Strait Islander indicator
- Mother's date of birth
- Father's date of birth
- Birth weight (in grams)
- Plurality – order (only available for multiple births e.g. twins)
- Plurality – total (only available for multiple births e.g. twins)
- Mother's occupation title

- Father's occupation title.

The disclosure will include any of the above information provided for other family members that is included in these records.

All other Principles continue to apply.

Conditions

The information is only to be used by SA NT DataLink for the creation of master linkage keys in the establishment of the Master Linkage File as part of the Data Linkage System. The exemption is provided on the condition that the personal information is only disclosed to, and accessed by, officers of SA Health located within SA NT DataLink.

SA Health remains responsible for the secure storage of personal information in line with the IPPs.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption will be reviewed by SA Health and the Privacy Committee three (3) years following its approval on 1 June 2011 unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

16 June 2011

Exemption - South Australian births and deaths datasets

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[6] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Office of Consumer and Business Affairs (OCBA) in the Attorney General's Department. It is an exemption from compliance with Principle 10, allowing OCBA to disclose personal information to the South Australian Northern Territory DataLink (SA NT DataLink).

[6] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

The personal information to be disclosed is from the South Australian births and deaths datasets and is limited to:

Death Dataset

- Unique record identifier (registration number)
- Names (all names where available including surnames, surnames at birth, given names and given names at birth)
- Date of birth
- Date of death
- Age at death
- Place of birth
- Place of death
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Full residential address, including geocodes, where available.

Birth Dataset

The following personal information to be used from the births dataset is limited to birth records within the data range 1/1/1999 to 31/12/2005.

- Unique record identifier (registration number)
- Names (all names where available including surnames, surnames at birth, given names and given names at birth)
- Full residential address, including geocodes where available
- Sex
- Date of birth
- Place of birth
- Mother's Aboriginal indicator
- Mother's Torres Strait Islander indicator
- Father's Aboriginal indicator
- Father's Torres Strait Islander indicator
- Mother's date of birth
- Father's date of birth
- Birth weight (in grams)
- Plurality – order (only available for multiple births e.g. twins)
- Plurality – total (only available for multiple births e.g. twins)
- Mother's occupation title
- Father's occupation title.

The disclosure will include any of the above information provided for other family members that is included in these records.

All other Principles continue to apply.

Conditions

The information is only to be disclosed to SA NT DataLink for use in the creation of master linkage keys in the establishment of the Master Linkage File as part of the Data Linkage System. The exemption is provided on the condition that the personal information is only disclosed to, and accessed by, officers of SA Health located within SA NT DataLink.

The OCBA remains responsible for the secure transfer and storage of personal information in line with the IPPs.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption will be reviewed by OCBA and the Privacy Committee three (3) years following its approval on 1 June 2011 unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

16 June 2011

D Exemption Granted – Housing SA and SA Police

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[7] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the South Australian Police (SAPOL) and Housing SA, a business unit of the Department for Families and Communities. It is an exemption from compliance with IPPs 8 and 10, allowing SAPOL and Housing SA to share personal information under a Ministerial Agreement between the Minister of Police and Minister for Families and Communities. The Ministerial Agreement aims to address crime and social disorder in South Australian Housing Trust Properties.

This exemption allows the use or disclosure of personal information in line with the Strategic and Operational Protocols (the Protocols) established under the Ministerial Agreement. The personal information covered by this exemption is collected and held by each agency through its mandated service provision.

All other Principles continue to apply.

Conditions

This exemption only applies to information used and disclosed under the Protocols. It is provided on the condition that the protocols be modified to ensure personal information about an individual shared under the Agreement will only be used for a purpose other than the purpose of collection, or disclosed to a third person, where:

- the person using or disclosing the information is authorised by the agency to use or disclose the information; and

- the individual has consented to the use or disclosure; or
- the person using or disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health, welfare or safety of the person who is the record subject or any other person; or
- the person using or disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the health and safety of members of the public; or
- the use or disclosure is required or authorised by or under law; or
- the use or disclosure is reasonably necessary (by or on behalf of an enforcement body) for one or more of the following:

[7] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

- the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
- 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 prescribed conduct;
- the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

It is noted that where use or disclosure is to prevent, detect or investigate a criminal offence or a breach of law, that this would include disclosures of personal information between SA Police and Housing SA where reasonably necessary to prevent damage to property, disorderly or violent conduct (towards a person or property) or conduct that would otherwise disturb the public peace. These uses or disclosures may include those necessary to substantiate or negate allegations made between community members about public disorder and disturbance of the public peace.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30).

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption will expire on 21 October 2011. An extension may be negotiated with the Privacy Committee prior to this date if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

23 December 2010

E Exemption Granted – Offender Management Plan

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[8] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the South Australian Police (SAPOL), the Department for Correctional Services (DCS), the Department for Families and Communities (DFC), the Attorney General's Department (AGD) and the Department of Health (SA Health). It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DFC, AGD and SA Health, to share case file information of serious offenders as part of the Offender Management Plan Pilot Program (Pilot Program).

The personal information to be shared is case file information and other personal information relevant to offenders included in the Pilot Program. The information is collected and held by each agency through its mandated service provision.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the Pilot Program in providing coordinated case management of selected serious offenders to reduce recidivism and promote community safety. This exemption also provides for the disclosure of relevant personal information to third party service providers necessary for the provision of targeted services to individual offenders under the Pilot Program.

All other Principles continue to apply.

Conditions

This exemption is conditional on the personal information shared through the Pilot Program only being used for the purposes of coordinated case management of selected serious offenders. It is also conditional on individual offenders being informed of their inclusion in the Pilot Program.

The exemption is restricted to information relevant to the coordinated case management of selected serious offenders.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30).

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

---

[8] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

Expiry

This exemption was approved by the Privacy Committee on 2 March 2011. It applies from the date of expiry of the previous exemption granted to the agencies participating in the Pilot Program (15 March 2011) for a further one (1) year or until the end of the Pilot Program whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

30 March 2011

F Exemption Granted – OCSAR Evaluation - Offender Management Plan

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[9] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Attorney General's Department and specifically the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information from the agencies participating in the pilot Offender Management Plan.

The personal information to be collected and used in the evaluation is:

- Family name and given name
- Address
- Ethnicity
- Date of birth
- Gender
- Drug use
- Health issues that impact on the participants' progress in the pilot
- Housing
- Education and employment
- Supervision by Corrections
- Number and type (major charge) of apprehension events prior to the pilot
- Number and type of apprehension events during the pilot
- Actions and interventions conducted as part of the pilot
- Participant response to case management.

The purpose of collection and use is to allow OCSAR to undertake an evaluation of the pilot Offender Management Plan.

All other Principles continue to apply.

Conditions

This exemption is conditional on OCSAR operating in accordance with the Offender Management Plan Information Sharing Protocol. This exemption is also conditional on participating offenders being informed of the use of their information for the evaluation of the pilot Offender Management Plan.

---

[9] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30).

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is provided for one year following its approval. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

26 July 2010

G Exemption Granted – OCSAR Evaluation Community Protection Panel

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[10] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Office of Crime Statistics and Research (OCSAR) of the Attorney- General's Department. It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information in the evaluation of the Community Protection Panel (CPP). The personal information to be collected and used in the evaluation relates to young offenders under the management of the CPP.

The personal information to be collected and used in the evaluation is:

- Name, date of birth, sex, ethnicity
- Court order imposed
- Health issues (i.e. drug use, physical and/or mental health) as they relate to case management and service provision
- Housing
- Education and employment
- Care and protection history
- Periods of detention
- Number of offences and most serious offence (based on major charge) prior to and during participation in the CPP
- Action plans/ services provided as part of the case management process
- Participant response to the case management process.

The purpose of collection and use is to allow OCSAR to undertake an evaluation of the Community Protection Panel.

All other Principles continue to apply.

Conditions

This exemption is conditional on OCSAR obtaining approval for the evaluation from the Department for Families and Communities Human Research Ethics Committee and the Aboriginal Health Research and Ethics Committee. It is also conditional on OCSAR ensuring that the outcome of the evaluation would not result in the disclosure of personal information to a third party in a form that would identify an individual offender or from which an individual offender would be reasonably identifiable.

[10] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30).

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption is provided for 18 months following its approval. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

8 October 2010

H Exemption Granted – OSCAR Evaluation Early Intervention Pilot Program

Exemption - OCSAR

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[11] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Office of Crime Statistics and Research (OCSAR) of the Attorney General's Department. It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information from the Drug and Alcohol Services South Australia's (DASSA's) Drug Diversion Line and offence data from the Justice Information System.

The information collected from the DASSA's Drug Diversion Line consists of referrals made by the South Australia Police and the Family Conference Team in the Courts Administration Authority.

The personal information to be collected and used in the evaluation is:

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)
- Date of birth (age)
- Gender
- Telephone contact details
- Information held on the Justice Information System about record-cases' contact with the criminal justice system.

The purpose of collection and use is to allow OCSAR to undertake an evaluation of the Early Intervention Pilot Program.

All other Principles continue to apply.

Conditions

This exemption is conditional on OCSAR obtaining approval for the evaluation from the South Australian Department of Health's Human Research Ethics Committee.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30).

---

[11] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption supersedes the previous exemption provided to OCSAR in relation to the Pilot Program. It is provided for four years following its approval. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

26 August 2010

Exemption - DASSA

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[12] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to Drug and Alcohol Services South Australia (DASSA) of the Department of Health. It is an exemption from compliance with Principles 2 and 10, allowing DASSA to collect personal information from the South Australia Police and the Family Conference Team in the Courts Administration Authority in relation to young persons suspected of alcohol related offences and the disclosure of that information to the Office for Crime Statistics and Research.

The personal information to be collected includes:

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)
- Date of birth (age)
- Gender
- Telephone contact details.

The purpose of collection and disclosure is to allow for the diversion of suspected young offenders to a health intervention through the Early Intervention Pilot Program and to facilitate the evaluation of that program by the Office of Crime Statistics and Research.

All other Principles continue to apply.

---

[12] *Cabinet Administrative Instruction 1/89 The Information Privacy Principles Instruction*

Conditions

This exemption is conditional on the provision of information on the nature of the referral and the health intervention diversion program to each young person who has been diverted to a program and their parents or guardians.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30).

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*.

Expiry

This exemption supersedes the previous exemption provided to DASSA in relation to the Pilot Program. This exemption is provided for four years following its approval. DASSA is to report to the committee on the operation of the Pilot Program two years after the approval of this exemption. The report should highlight any privacy issues raised or complaints received in the operation of the Pilot Program. An extension to this exemption may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

26 August 2010

I Exemption Granted – Information Sharing Guidelines

Exemption

In accordance with Clause 4 of the Proclamation dated 17 May 2001 under which the Privacy Committee was established, the Privacy Committee grants the following exemption from compliance with Information Privacy Principle (IPP) 10(b), issued under *Cabinet Administrative Instruction 1/89 "The Information Privacy Principles"* .

This exemption applies to agencies that are required to observe the *Information Sharing Guidelines for promoting the safety and wellbeing of children, young people and their families* (the Guidelines).

IPP 10(b) provides that *an agency should not disclose personal information about some other person to a third person unless the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious* ***and imminent*** *threat to the life or health of the record subject or some other person* (our emphasis)*.*

This exemption authorises the disclosure of personal information without the consent of the record subject where the person disclosing the personal information does not have or has no reasonable grounds to believe that a threat to the life or health of a person who is under 18 years of age is *imminent,* insofar as the word "imminent" is generally understood to mean *"immediate*".

The effect of the variation is to remove the words "and imminent" from IPP 10(b).

In all other respects the requirements of the IPPs continue to apply and must be observed. In particular, the person making the disclosure must believe on reasonable grounds that the threat is "serious", as required by IPP 10(b), according to the ordinary meaning of that word and in the context of any particular special needs or vulnerabilities of the juvenile record subject.

To avoid doubt, this exemption does not apply to personal information

- that is required or permitted to be disclosed by law; or
- for which the law prohibits disclosure

Compliance

The Chief Executives of agencies required to observe the Guidelines must ensure compliance with this exemption.

Further Conditions

This exemption is also conditional on Chief Executives ensuring the proper implementation of the Guidelines within agencies, particularly:

- the recording of decisions where personal information was disclosed without consent;

- the introduction of staff / volunteer induction on the application of the Guidelines;

- the adoption of appropriate protocols for gaining consent from clients for disclosing personal information.

The Office of the Guardian is responsible for reporting to the Privacy Committee on the implementation of the Guidelines within twelve (12) months of the approval of this exemption.

Expiry

This exemption will be reviewed by the Office of the Guardian and the Privacy Committee two (2) years after its approval at the Privacy Committee's meeting on 6 April 2011. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

29 June 2011