Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2012

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 2012

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
email: 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 Michael O'Brien MP
MINISTER FOR THE PUBLIC SECTOR

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 2012. 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

28 September 2012

Table of Contents

1 Introduction

The first Privacy Committee of South Australia was appointed in 1983. In 1989, after Cabinet approval of the *Information Privacy Principles Instruction* (IPPs) a year earlier, the Privacy Committee was established by proclamation and a new Privacy Committee of South Australia was appointed.

Since 1989, the Privacy Committee has been primarily responsible for overseeing the implementation and maintenance of the IPPs by South Australian Government agencies. It has also played an important role in promoting privacy protection in general and ensuring that impacts on privacy are considered in the development of Government initiatives and State and National law reforms. The functions of the Privacy Committee include making recommendations to the Government or any person or body as to measures that should be taken to improve the protection of individual privacy, receiving written complaints concerning violations of individual privacy, and granting exemptions.

Privacy remains important to the community. Recent Australian research indicates that people are concerned about their privacy and particularly about their privacy online. A survey undertaken by the University of Queensland found that over 90% of Australian respondents support laws to protect their privacy and allow them to control the use of their personal information online[1]. The Privacy Committee notes that many citizens expect and assume a level of privacy protection that is not always sufficiently covered by various South Australian laws. There are significant inconsistencies and gaps in privacy protection across Australia and between the public and private sectors[2].

South Australia remains one of only two Australian jurisdictions without information privacy law regulating its public sector. The Privacy Committee remains committed to working with Government to introduce information privacy law in South Australia. To this end, the Committee continued to support the Minister and State Records during 2011-12 with advice and guidance on the development of information privacy legislation for the South Australian public sector.

The challenges facing individuals in the protection of their privacy have changed significantly since the Privacy Committee was established. Technological advances in the areas of communications and the mobility and sharing of information have intensified and increased the risk to personal information. Over the past few years, the number of Smartphone users has increased dramatically and there is an increase in demand for more Government services to be delivered online. There has also been a further increase in online fraud and cybercrime and many high profile breaches of personal information have been reported, particularly in the private sector.

---

[1] Online Privacy Survey, University of Queensland, http://cccs.uq.edu.au/personal-information-project

[2] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice, Report 108*, 2008, pp 161-187 and p 496

Public sector agencies are not immune to these challenges. They have to remain diligent to ensure they are complying with their obligations under the IPPs and appropriately managing the risks to personal information. The Privacy Committee advises agencies that undertaking a Privacy Impact Assessment will assist in ensuring that privacy risks have been adequately addressed when developing new information technology systems, making changes to older systems, or implementing any new government initiative that involves the handling of personal information.

Agencies need to give early consideration to impacts of their actions on the privacy of personal information or their obligations under the IPPs.

The Privacy Committee notes that a number of reforms at both the State and national level, which include measures that are aimed at improving privacy protections, have progressed during 2011-12.

During the year, the Committee provided advice and recommendations on information privacy oversight in relation to the establishment of two national regulatory bodies initiated by the Council of Australian Governments. These bodies will be established for the introduction of national rail safety regulation and the national regulation of heavy vehicles. The Committee's experiences in responding to these national regulatory schemes highlighted the need for early consideration and consultation on the privacy oversight issues in the development of national reform proposals.

The Privacy Committee continued activities related to its role in receiving privacy complaints, responding to privacy enquiries and granting exemptions from the IPPs. During the reporting year, the Privacy Committee extended or granted 19 exemptions from the IPPs to State Government agencies (see item 3.7), concluded 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 148 enquiries from the public and State Government agencies, which is the same number of enquiries handled in 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 2012. 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 are 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.

Principles 1-3 – Collection

Personal information must be collected legally and fairly. It should not be collected unnecessarily. Individuals should be told the purpose for which their personal information is being collected and how it will be used, and to whom the agency usually discloses it. Personal information should be kept up-to-date, complete and accurate.

Principle 4 – Storage

Agencies 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.

Principle 5-6 – Access and Correction

Individuals are able to apply for access to their own personal information in accordance with the *Freedom of Information Act 1991* and can seek to have it corrected if they consider it to be incomplete, incorrect, out-of-date or misleading.

Principles 7-10 – Use & Disclosure

Personal information should only be used for the purpose for which it was collected, and it should not be disclosed to a third party unless:

- the person has expressly or impliedly consented;
- it is required to prevent a serious threat to the life or health of someone;
- it is required by law; or
- it is required for enforcing a law, protecting public revenue, or protecting the interests of the government as an employer.

The IPPs are not intended to prevent disclosure of personal information where it is in the public interest to do so, such as a serious threat to the life or health of a child or any other person, and does not prevent the disclosure of information where there is lawful reason to do so.

The Information Privacy Principles Instruction can be accessed 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 which was 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.

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 2011-12, the Privacy Committee initially reported to the Hon Gail Gago MLC, Minister for Public Sector Management and, from October 2011, to the Hon Michael O'Brien MP, Minister for the Public Sector.

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, Department of the Premier and Cabinet
- Bernadette Quirke, Legal Counsel, Crown Solicitor's Office, Attorney-General's Department
- Nancy Rogers, Manager, Research, Department for Communities and Social Inclusion
- Andrew Stanley, Director, Policy, Legislation and Research, Department of Health and Ageing

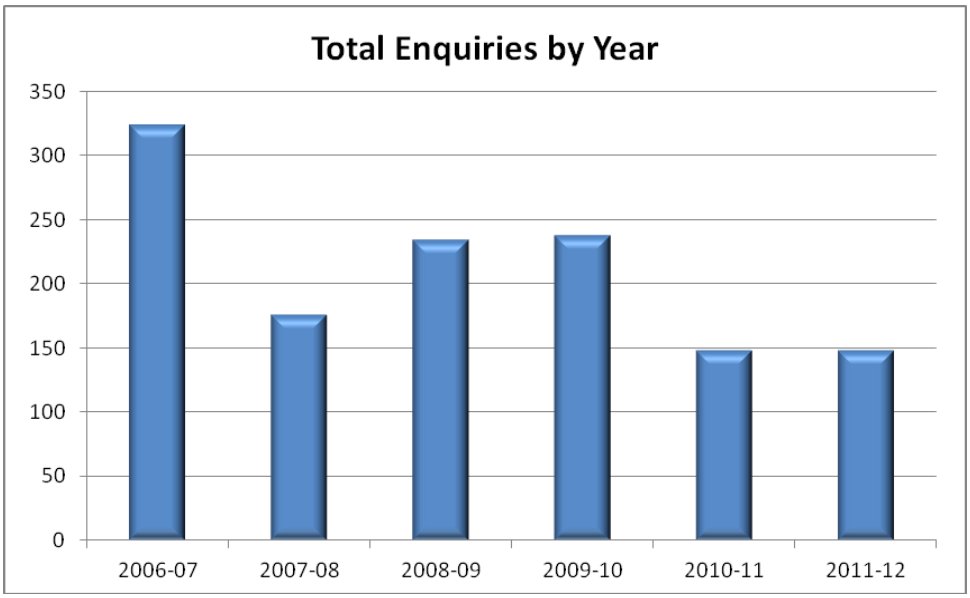
The term of appointment for each of the current members expires on 5 December 2012.

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.

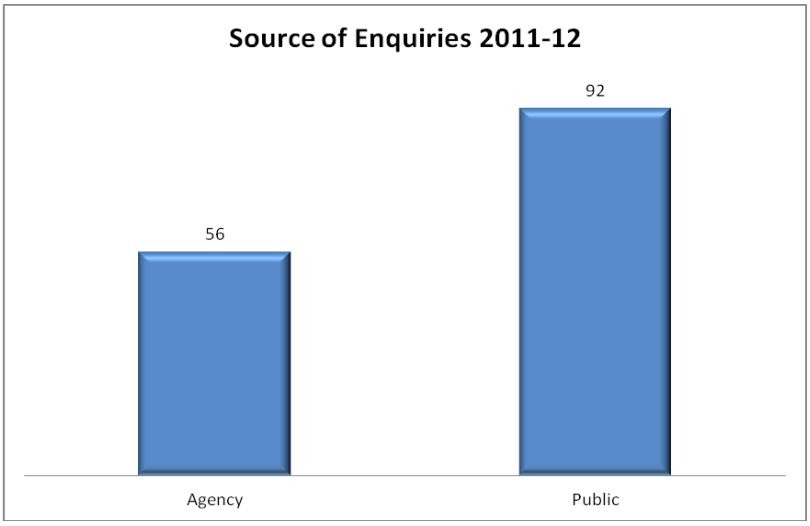
2.2.4.1 Privacy Enquiries

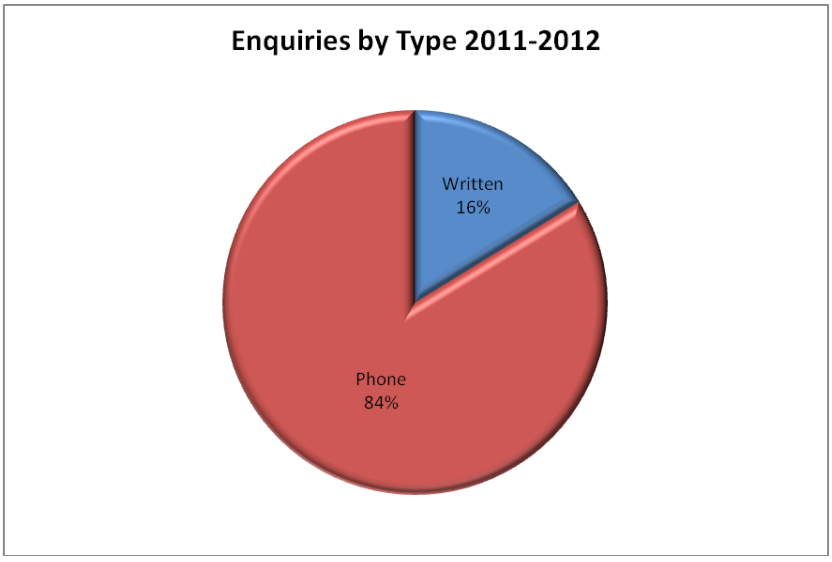
During the reporting year, State Records responded to 148 telephone and email enquiries from the public and State Government agencies relating to all aspects of privacy of personal information. This is the same number of enquiries reported in the previous year.

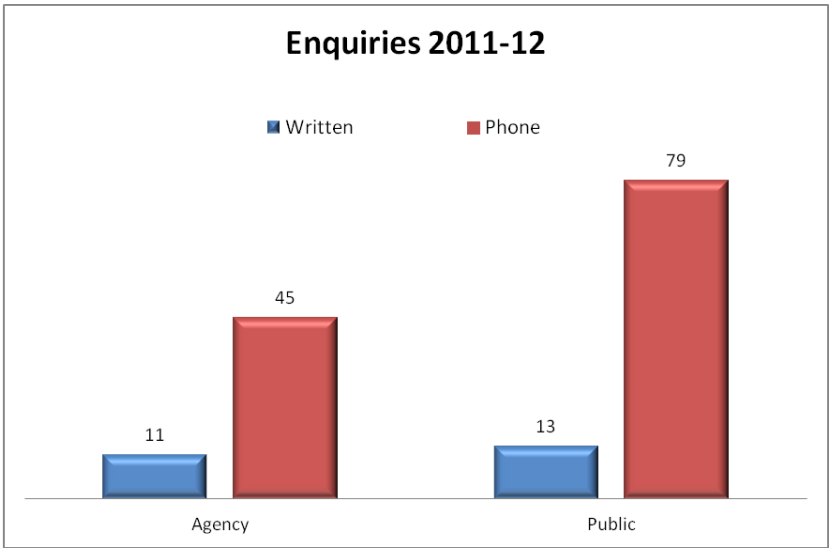


The number of enquiries received from the public increased by 21%, from 76 reported last year to 92 for 2011-12. The number of enquiries received from

State Government agencies decreased by 22%, from 72 reported last year to 56 for 2011-12.







2.2.4.2 Privacy Training

State Records conducted a Privacy Awareness session for State Government employees during the year. Privacy awareness is also included in the curriculum for the nationally accredited Certificate III in Recordkeeping, as well as the online e-resource network initiative (ERNI), which are 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. Only non-government members of the Privacy Committee are 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 7 occasions. Where possible, 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.

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

In 2011, the Government of South Australia published its second update to South Australia's Strategic Plan. The updated plan reflects the input and aspirations of communities for how to best grow and prosper and how we can balance our economic, social and environmental aspirations in a way that improves our overall wellbeing, and creates even greater opportunities. The constitution of the Privacy Committee meets the new Target 30 (Priority: Our Community) to 'increase the number of women on all State Government boards and committees to 50% on average by 2014, and maintain thereafter by ensuring that 50% of women are appointed, on average, each quarter'. During the reporting year the Privacy Committee maintained a 50% female membership.

The activities of the Privacy Committee contribute to the achievement of Target 32 of South Australia's Strategic Plan. Target 32 'customer and client satisfaction with government services' is part of the broader goal of demonstrating strong leadership working with and for the community within the 'Our Community' priority. 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.

In February 2012, the Premier announced seven strategic priorities which are those areas from the plan the Government has chosen to focus on. Those strategic priorities are Creating a Vibrant City; Safe Communities, Healthy Neighbourhoods; An Affordable Place To Live; Every Chance For Every Child; Growing Advanced Manufacturing; Realising The Benefits Of The Mining Boom For All; and Premium Food And Wine From Our Clean Environment.

These priorities are to be achieved through three approaches to government: a culture of innovation and enterprise; sustainability; and a respect for individuals with a reciprocal responsibility to the community.

The work of the Privacy Committee, in particular its endorsement of the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families*, is complimentary to and supports the implementation of the priorities and associated approaches in relation to Safe Communities, Healthy Neighbourhoods and Every Chance for Every Child.

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 concerning national consistency in privacy law in Australia, privacy and national regulatory reform initiatives and Smartphone applications.

The Committee continued to support the Minister and Government in the development of information privacy legislation for the South Australian public sector. The Committee specifically provided advice to the Minister and State Records to support the establishment of a project to develop the legislation. The Committee expects that public consultation on a draft Information Privacy Bill will occur in 2012-13.

The Privacy Committee also provided advice to Government agencies and 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

Significant progress was made in national privacy law reform during the year particularly in regard to reforming the Commonwealth *Privacy Act 1988*. On 23 May 2012, the Australian Government introduced the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*. The Bill was the latest development in the Government's response to the Australian Law Reform Commission's (ALRC) *Report 108* on Australian privacy law and practice.

The Bill is focussed on three key reforms. The first is the introduction of a revised set of Australian Privacy Principles to replace the two existing sets of privacy principles in the Privacy Act. The second is to revise the credit reporting provisions which will make it easier for individuals to access and correct their credit information and allow banks and financial institutions to see an increased amount of information about individual credit histories. The third is to increase the powers of the Commonwealth Privacy Commissioner to enforce the Privacy Act.

The Bill was referred to two Parliamentary Committees for further consideration. These included the House of Representatives Standing Committee for Social Policy and Legal Affairs and the Senate Committee for Legal and Constitutional Affairs. Public consultation on the Bill is being facilitated by these Committees and it is expected that further development of these reforms will occur in 2012-13.

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.

On 26 June 2012, the Australian Parliament passed the *Personal Controlled Electronic Health Records Act 2012*. The Act established the governance and authority for the development and oversight of the Personally Controlled Electronic Health Records (PCEHR) System.

The aim of the proposed system is to give all Australians the option to sign up for a PCEHR. The PCEHR system will provide individuals the opportunity to see their health information when and where they need it and to share this information with relevant healthcare providers. Healthcare providers see it as a potential for better communication to support quality healthcare services. This includes the potential for more efficient and accurate transfer of health information across the health sector.

The Privacy Committee has kept itself informed of developments in the PCEHR system and governing legislation throughout the year. It noted the release of the Privacy Impact Assessment undertaken on the PCEHR system in late 2011. The Committee specifically noted that the lack of information privacy legislation in South Australia and Western Australia added complexity to the establishment of privacy provisions under the PCEHR legislation.

The protection of personal information within the PCEHR system is essential to its success. A key element of this protection will be the effective handling of information privacy complaints. During 2011-12, the Privacy Committee participated in discussions to establish a privacy complaints handling framework for the PCEHR System with the Office of the Australian Information Commissioner, the Australian Government as the System Operator for the system, and other State and Territory privacy and health record complaint handling bodies.

The Privacy Committee will continue to keep itself informed of the development and implementation of the PCEHR System as it progresses in 2012-13.

3.2.1.4 National Heavy Vehicle Regulation

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

The proposed NHVL 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, will apply to all vehicles over 4.5 tonnes, and come into effect in January 2013.

The Privacy Committee provided further advice to the Department of Planning, Transport and Infrastructure in November 2011 on options for the information privacy arrangements under the proposed laws to support the State's response to national consultations.

One of the concerns of the Committee in the approach to establishing national regulatory schemes such as the NHVL is the potential for further fragmentation and complexity of privacy regulation in Australia. The Committee has

recommended as far as possible a consistent approach to such schemes and has worked with the other privacy authorities in Australia to raise this issue with the Council of Australian Governments.

3.2.1.5 National Rail Safety Regulator

A further National Regulatory Scheme came to the attention of the Committee during 2011-12. The Rail Safety National Law (RSNL) will establish a scheme of rail safety oversight across Australia to replace existing State and Territory based regulation. The Law will also establish a National Rail Safety Regulator to provide oversight of rail safety under the Law. South Australia was selected as the host jurisdiction for the Regulator.

The Privacy Committee was consulted on the proposed information privacy arrangements for the scheme. As the Regulator is to be hosted by South Australia it was proposed that State administrative oversight laws would be applied to the Regulator under the RSNL. The laws include the *State Records Act 1997*, the *Freedom of Information Act 1991*, the *Ombudsman Act 1972* and the *Public Finance and Audit Act 1987*. The current absence of information privacy laws in South Australia prevented the immediate adoption of a similar approach for privacy oversight. The Privacy Committee has continued to work with the RSNL project office to ensure the development of appropriate privacy policies and practices for the Regulator.

3.2.1.6 National Mental Health Statement of Rights and Responsibilities

In January 2012, the Privacy Committee participated in consultation on the National Mental Health Statement of Rights and Responsibilities (Statement).

The Statement is intended for implementation in all jurisdictions and will be incorporated into mental health operations, policy, legislation, prevention, promotion, education, quality improvement and workforce development initiatives. The Statement directly recognises that mental health consumers and carers have the right to privacy and confidentiality and the right to be considered capable of making a decision.

The Privacy Committee provided comments on the Statement as it referred to the privacy rights of individuals. It provided specific comment on the definition of privacy under the statement and on the right of individuals to access their personal information.

3.2.1.7 Statutory Cause of Action for Invasion of Privacy

In September 2011, the Australian Government released an issues paper for public consultation on the establishment of a Statutory Cause of Action for Invasion of Privacy under Commonwealth law. The issues paper considered the recommendation of the Australian Law Reform Commission (ALRC) in its Report 108, as well as recommendations from the Victorian and New South Wales Law Reform Commissions.

A statutory cause of action would provide individuals with the right to take legal action for serious invasions of privacy. The key element of the ALRC's proposal was that an action can be brought only where such invasions were highly offensive to a reasonable person of ordinary sensibilities, in circumstances where

there was a reasonable expectation of privacy. It also provided for the balancing of the right to privacy with other important rights such as the right to free expression and actions in the public interest.

The Privacy Committee made a submission in response to public consultation on the issues paper, which broadly supported the ALRC's proposed model for creation of a statutory cause of action.

3.2.2 Meetings and seminars

Throughout the year, the Privacy Committee was represented at various meetings, seminars and forums, including:

- one meeting of the Asia Pacific Privacy Authorities (APPA); and
- two meetings of the Privacy Authorities of Australia (PAA).

3.2.2.1 Asia Pacific Privacy Authorities

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.

The Privacy Committee was represented at the meeting of APPA held in Melbourne on 1 to 2 December 2011. The meeting considered issues including:

- privacy law reforms in the Asia Pacific region
- video surveillance and privacy
- information privacy impacts of cloud computing
- privacy impacts of biometrics technology
- 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 2011 and 11 May 2012.

PAA membership consists 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 September 2011 meeting considered privacy issues in relation to:

- National privacy law reforms
- National regulatory schemes
- Body scanning in Australian airports

- National Identity Security Strategy
- Cooperation between PAA Members.

The May 2012 meeting included:

- National Regulatory Schemes
- National Teacher Workforce Dataset Project
- National Identity Security Strategy – Document Verification Service
- Personally Controlled Electronic Health Records System.

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 Adelaide Fare Collection System (MetroCard)

In July 2011, the Privacy Committee was consulted on the implementation of the Adelaide Fare Collection System (AFCS) by the Department of Planning, Transport and Infrastructure (DPTI), formerly the Department of Transport, Energy and Infrastructure. The AFCS is the IT system that supports South Australia's new transport smartcard, known as Metrocard, which is being introduced by the Government across the State's public transport network.

Individuals will be able to register their Metrocard on the AFCS allowing them to replace the card if lost, add credit online and receive information about public transport services. Individuals will have the option to use a Metrocard without the need to register. However, some benefits such as card replacement are not available if the card is not registered. Public transport users will also have the option of not using a Metrocard at all, as magnetic strip tickets for single and daily trips will be retained.

The Committee is encouraged by the design of the Metrocard and the associated AFCS as it appears to be less privacy invasive, offering individuals a range of options for unregistered travel, compared with transport smartcard systems implemented in other Australian jurisdictions.

The Privacy Committee made a number of recommendations to DPTI aimed at assisting the development of privacy policies for the AFCS. A key recommendation was that the privacy policy should be easily accessible and understood by the public and available to be viewed or accessed prior to the collection of personal information.

The Committee was further consulted on the privacy arrangements for the Metrocard and the AFCS in early 2012 in preparation for the anticipated launch of the Metrocard in late 2012.

3.3.2 SA NT DataLink

SA NT DataLink is the operational body of an unincorporated joint venture, comprising SA and NT Government and non-government agencies. Responsible for the development and operation of both an SA and NT population Master Linkage File (MLF), SA NT DataLink discovers and records links between common clients from disparate administrative datasets. Identifying variables such as name, date of birth and address, are only ever provided to SA NT DataLink for determining links. Once linked into the MLF an individual's identity is de-identified by a unique and random code, allowing researchers to merge and analyse multiple de-identified source data.

SA NT DataLink's service pools de-identified data from multiple government and non-government agencies. This allows population level health, social, education and economic research and evidence-based policy development to be undertaken whilst minimising risks to individual privacy when compared to traditional sample based research using identified data.

Data linkage through SA NT DataLink is supported by the Privacy Committee with a number of exemptions, primarily around the governance of data. This includes obtaining approval from a South Australian Government Human Research Ethics Committee (HREC).

SA NT DataLink continued to progress during 2011-12, with the Housing SA dataset being approved for inclusion in the MLF. In addition, the Privacy Committee renewed other exemptions from the IPPs to facilitate the development and maintenance of the MLF. 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 Appendices APPENDIX E and 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 is essential for the Government to achieve streamlined integrated and accessible services to citizens and business. Identity security management has strong links with information privacy protection when considering the potential for identity theft or fraud.

While identity crime is not new, rapidly evolving technology continues to provide improved opportunities for identity theft and fraud. In 2010-11 the Australian Bureau of Statistics estimated that Australians lost $1.4 billion due to personal fraud.

State Government agencies hold information critical to an individual's proof of identity, such as driver's licences, birth and marriage records and other 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 participated in State consultations with the Commonwealth on an updated National Identity Security Strategy and Document Verification Service.

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[3]. 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 finalised a review of the development of applications for mobile devices by Government agencies. It commenced reviewing its guidance in relation to privacy and the Internet to take into account developments in this technology. It is expected that new guidance will completed and published during 2012-13.

3.3.6 Australian Early Development Index

During the year, the Privacy Committee received an application from the Department for Education and Child Development (DECD) for exemption from the IPPs for the disclosure of personal information to the Commonwealth Department of Education, Employment and Workplace Relations (DEEWR). The disclosure was to allow for the pre-population of the Australian Early Development Index (AEDI) survey.

AEDI is a national progress measure for the National Early Childhood Development Strategy, an initiative of the Council of Australian Governments and the key measure of an agreed target of South Australia's Strategic Plan. It involves collecting information to help create a snapshot of children's development in communities across Australia. Teachers complete a survey for each child in their first year of full-time school. The survey measures five key areas of early childhood development:

- physical health and wellbeing
- social competence
- emotional maturity
- language and cognitive skills (school-based)
- communication skills and general knowledge.

The Privacy Committee provided advice and recommendations on the process for the collection of information for the AEDI. This included the process for the collection of information by South Australian public schools and the disclosure of enrolment information held by DECD to the Social Research Centre (SRC). The SRC is a research services company contracted by the Australian Government to conduct the AEDI survey.

The Privacy Committee was particularly concerned about the adequacy of the process for parental consent for the collection of a child's information as part of the AEDI. It was the Committee's view that in order to provide personal information for the purposes of pre-population of the AEDI survey DECD would require informed consent. However, the DECD consent letter asked parents to inform the school if they did not want information about their child collected. The

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

Committee did not consider this process gave adequate opportunity to provide informed consent. Further, the Committee believed that DECD should have taken the opportunity to seek informed consent via the parental consent letter.

The Committee did not support the submission for DECD to disclose identified personal information to the Commonwealth. It was the Committee's view that de-identified data was all that was required for the primary purpose of the survey, and that no identified data should be collected.

3.3.7 Summary Offences Act – Filming Offences

In late November 2011, the Attorney-General released a consultation paper with an exposure draft Bill to amend the *Summary Offences Act 1953.* The proposed amendments are to create new offences intended to combat humiliating and degrading filming and the non-consensual distribution of invasive images.

The Privacy Committee provided a response to the consultation paper in January 2012 that supported the introduction of further laws. The Committee recommended that the introduction of the laws be supported by a comprehensive public promotion and education campaign particularly targeting teenagers and young adults.

A revised Bill to amend the *Summary Offences Act 1953* was tabled in Parliament in May 2012 for further public comment. It is expected that the Bill will be considered by Parliament in 2012-13.

3.3.8 Young Offenders

In May 2012, the South Australia Police (SAPOL) sought an exemption from the IPPs to allow the disclosure of young offenders personal information to their parents or guardians where a youth is formally cautioned; issued with an expiation notice; reported; or under 10 years of age.

The Committee, when considering the request, was of the opinion that an exemption from the IPPs may not be required as disclosure of the information may be warranted under relevant law. The Committee subsequently recommended that SAPOL seek legal advice on the issue. At the close of the reporting year, the Committee had not received any further information from SAPOL.

3.3.9 BASS Ticketing

In June 2012, BASS South Australia sought an exemption from the IPPs to allow the disclosure of event specific patron lists to publicly funded arts companies.

BASS South Australia is operated by the Adelaide Festival Centre Trust and is the exclusive ticketing agency for all Adelaide Festival Centre venues. BASS South Australia has exclusive ticketing arrangements with the publicly funded arts companies that perform in Adelaide Festival Centre venues.

The purpose of the submission was to allow disclosure of event specific patron listings so that the publicly funded arts companies could contact their patrons to verify the patron's email and contact preferences relative to that company.

The Committee was continuing its consideration of this submission at the close of the reporting year.

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 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 Committee is also represented on the South Australian Government's ICT Security and Risk Steering Committee.

The Privacy Committee was also represented on the South Australian Government's Identity Security Management Group.

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 on their compliance with the IPPs and in some cases this is a condition of an exemption. See section 3.3 for further information. In addition, under the terms of the IPPs, the Committee may on its own initiative appoint a person to investigate or assist in the investigation of the nature and extent of compliance with the principles. One investigation was carried out during the year.

3.5.1 Privacy Breaches

The Privacy Committee considered one breach of the IPPs during the year. The breach involved a confidential Families SA file that was left in a filing cabinet that was subsequently sold at auction. The file was found by a member of the public and passed on to a media outlet and the breach was then reported in the media. The file was ultimately returned to Families SA.

An investigation was conducted by an officer from State Records who considered Families SA practices in relation to the management of personal information under the *State Records Act 1997*. The results were reported to the Privacy Committee.

The investigation highlighted breaches to Families SA's Code of Fair Information Practice, in particular Principle 2 (Use and Disclosure) and Principle 4 (Data Security). It found that Families SA did not take reasonable steps to ensure the personal information in the file was accessed only by authorised individuals and as a result personal information was inadvertently disclosed.

As a result of the findings Families SA committed to revising its policies and procedures in relation to record security taking into account its obligations under the IPPs, especially relating to the relocation of office furniture. The agency has

now issued specific instructions to staff on the handling of records when relocating office furniture. The Privacy Committee will seek an update on Families SA's compliance with the principles during 2012-13.

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 the agency's opinion on what took place and 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 its 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 Australia 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 authorities. While there is no legislated or administrative privacy regime that applies to these organisations, the Committee has previously worked with both of them to resolve privacy complaints and improve their practices when handling personal information.

During the reporting year there were two formal complaints received, with both complaints concluded during the year. A summary of these complaints is outlined in the table below.

3.6.1 Complaints Concluded Summary Table

	Respondent Organisation	Information Privacy Principle (IPP)	Outcome
1	Government Dept	IPP 10 – Disclosure of personal information	Agency reviewed its practices to ensure compliance with the IPPs
2	Government Dept	IPP 10 – Disclosure of personal information on website	Agency removed personal information from website

3.6.2 Local Government complaints

Although the IPPs apply only to public sector agencies, the Privacy Committee received a range of enquiries relating to breaches of personal information in

Local Government authorities during the year but received no formal complaints. Of the enquiries received, a number related to the publication of personal information on Local Government authority websites. These enquiries highlighted the need for Local Government authorities to properly inform individuals of the authority's legal obligation to make certain information publicly available in line with best practice in information privacy protection.

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 Committee considers that 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, nine new exemptions were approved and ten existing exemptions were renewed. Of the 19 exemptions, two related directly to specific research projects and eight related to the SA NT DataLink data linkage project. Following is a summary of each of the requests for exemption.

3.7.1 SA NT DataLink

The Privacy Committee dealt with two submissions from SA NT DataLink during the year seeking an extension or new exemption 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 and operation of both an SA and NT population Master Linkage File (MLF).

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 MLF, with individual's identity de-identified by a unique and random code. The exemptions related to the following government datasets:

- Housing SA dataset
- Families SA dataset
- Public schools enrolment dataset
- South Australian Cancer Registry
- Public hospital inpatients morbidity dataset
- Emergency department dataset.

See 3.3.2 for more information on the SA Data Linkage Project and Appendices APPENDIX E and APPENDIX H for the full text of the exemptions.

3.7.2 Housing SA and SAPOL Ministerial Agreement

In November 2010, the Privacy Committee granted an exemption from IPPs 8 and 10 to the South Australia Police (SAPOL) and Housing SA. The exemption

was to permit use and disclosure of personal information under a Ministerial Agreement promoting cooperation between the agencies to address crime, and social disorder in South Australian Housing Trust properties.

In October 2011, the Privacy Committee renewed the exemption for a further three years. The exemption permits the exchange of personal information between the agencies where it is 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 – Pilot Program

In December 2011, the Committee granted a further twelve month exemption from IPPs 2, 8 and 10 to allow for information sharing between agencies through a pilot program of the South Australia Offender Management Plan. The agencies are the South Australia Police, the Department for Correctional Services, the then Department for Families and Communities, the Attorney General's Department and the then Department of Health. The exemption was later amended to include the Department of Further Education, Employment and Training as an agency participating in the pilot program, and to recognise the addition of a second pilot site in the South Coast region.

The purpose of the Offender Management 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 offenders selected to participate in the pilot program and conditional on those offenders being informed of their inclusion in the pilot program.

See APPENDIX C for the full text of the exemptions.

3.7.4 Offender Management Plan – OCSAR Evaluation

In September 2011, the Privacy Committee renewed an exemption for a further twelve month allowing the Office of Crime Statistics and Research (OCSAR) to collect and use personal information as part of an evaluation of the pilot program of the Offender Management Plan. 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 C for the full text of the exemption.

3.7.5 Offender Management Plan – Research Project

In December 2011, the Committee granted an exemption to agencies participating in the pilot program of the Offender Management Plan to allow the use and disclosure of personal information for a research project examining the information sharing practices of the pilot program. The exemption is subject to a number of conditions, including that it receive approval from a Human Research

Ethics Committee. The research project is to be carried out under the supervision of the South Australia Police and Flinders University.

See APPENDIX C for the full text of the exemption

3.7.6 Aboriginal Courts and Conferences – OCSAR Evaluation

In December 2011, the Privacy Committee considered a submission from OCSAR seeking an exemption from the IPPs to permit the use of personal information as part of a study of re-offending in relation to four South Australian Aboriginal sentencing courts and conferences.

The study was one part of an Australian Government initiative evaluating a number of justice programs to identify best practice approaches to tackling crime and justice issues in Indigenous communities. The findings of the re-offending study will provide an evidence base for future national Indigenous justice initiatives.

On 12 December 2011, the Privacy Committee granted an exemption from IPPs 2 and 8 to OCSAR to collect and use personal information without consent in the conduct of the evaluation.

See APPENDIX F for the full text of the exemption.

3.7.7 Collection of Social, Family or Medical History

On 7 December 2011, the Privacy Committee considered and approved the renewal of exemptions from IPP 2 granted to the Department for Health and Ageing, formerly the Department of Health, and the Department for Communities and Social Inclusion to permit the collection of a third party's personal information as part of a health consumer's social, family or medical history.

The exemption specifically permits the collection of health information from a health consumer about a third party without consent when both of the following circumstances are met:

- The information is necessary to provide a health service directly to a consumer.
- The third party's information is relevant to the social, family or medical history of that consumer.

In granting the exemptions to both departments the Privacy Committee considered the public interest in permitting the collection of third party information in order to provide continuing, comprehensive and quality health care for consumers, and determining better public health outcomes.

See APPENDIX G for the full text of the exemption.

3.7.7 Seniors Card Holders

In April 2012, the Privacy Committee considered and later approved a submission from the Department for Health and Ageing which sought an exemption from the IPPs to disclose the personal information of Seniors Card holders to the Department of Planning, Transport and Infrastructure (DPTI). The personal information was to be disclosed without the consent of Seniors Card holders to allow for the registration of Seniors Cards on the Adelaide Fare

Collection System. This was required as the Department for Health and Ageing (DHA) was issuing new Seniors Cards that will double as transport smartcards in line with the introduction of the Metrocard. Registration of the new Seniors Cards on the Adelaide Fare Collection System will allow Seniors Card holders to access all levels of DPTI customer service in relation to the new cards.

The Privacy Committee approved a once only exemption to DHA to allow the disclosure of personal information of existing Seniors Card holders to DPTI. Two related exemptions were approved for DPTI. One of these was a once only exemption allowing DPTI to collect the personal information of Seniors Card holders disclosed by DHA and the other was an ongoing exemption allowing DPTI to use the personal information disclosed by DHA in order to provide Seniors Card holders with all levels of DPTI customer service.

Consent will be sought from new Seniors Card holders to allow DHA to disclose their personal information to DPTI.

See Section 3.3.1 for more information on the Metrocard and AFCS.

See APPENDIX I for the full text of the exemption.

3.7.8 Intervention Orders and the Intervention Response Model

In June 2012, the Privacy Committee considered and later approved a submission from the Office of Crime Statistics and Research (OCSAR) seeking an exemption from the IPPs to permit the collection, use and disclosure of personal information without consent for the purposes of an evaluation of the implementation of the *Intervention Orders (Prevention of Abuse) Act 2009* (the Act). The exemption permits the disclosure of personal information by the Courts Administration Authority and the South Australia Police to OCSAR. The exemption also permits OCSAR to collect that information and use it for the purposes of the evaluation of Intervention Orders and the Intervention Response Model operating under the Act.

See APPENDIX J for the full text of the exemption.

Appendices

APPENDIX 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

APPENDIX 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.

APPENDIX C Exemption Granted – Offender Management Plan Pilot Program

Exemption – Office of Crime Statistics and Research

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 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 Offender Management Plan (OMP) Pilot Program.

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

- Family and given name
- Address
- Ethnicity
- Date of birth (age)
- Gender
- Drug use
- Health issues that impact on participants' progress in the pilot
- Housing
- Education and employment
- Supervision by Community Corrections
- Number and type (major charge) of apprehension events prior to and during the pilot
- time spent in custody prior to and during the OMP pilot
- Actions/interventions conducted as part of the case management process
- Participant response to the case management process
- Results of criminogenic needs assessments
- Results of Self-Appraisal Questionnaires completed.

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

All other Principles continue to apply.

Conditions

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

This is exemption is also conditional on the approval of the evaluation by a Human Research Ethics Committee constituted and acting in compliance with the *National Statement on Ethical Conduct in Human Research*.

[4] *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 or until the end of the OMP 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

15 September 2011

Exemption – SAPOL, DCS, DCSI, AGD, SA Health & DFEEST

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.

This exemption applies to the South Australian Police (SAPOL), the Department for Correctional Services (DCS), the Department for Communities and Social Inclusion (DCSI), the Attorney General's Department (AGD), the Department of Health (SA Health) and the Department for Further Education, Training and Employment (DFEEST). It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, AGD, SA Health and DFEEST, 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

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

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) and the Information Security Management Framework (ISMF). Participating agencies must specifically ensure that:

- Steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse
- Personal information is kept in a secure area within participating agencies
- Personal information is protected during transit; electronic information should be encrypted and password protected and physical files should not be left unattended in an insecure environment.
- Access to personal information is on a strictly need-to-know basis. Personal Information collected under the Pilot Program should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under a participating offender's case management plan, delivering services to the offender as an existing client or where otherwise allowable under IPPs 8 and 10.

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 exemption approved by the Privacy Committee on 2 March 2011. It applies from the date of its approval until 1 November 2012 or 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

12 December 2011

Exemption – SAPOL, DCS, DCSI, AGD, SA Health & DFEEST

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 South Australia Police, the Department for Correctional Services, the Department for Communities and Social Inclusion, the Attorney General's

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

Department, the Department of Health and the Department of Further Education, Employment and Training. It is an exemption from compliance with Principles 8 and 10, allowing personal information to be disclosed by the agencies participating in the Offender Management Plan (OMP) Pilot Program to a researcher from Flinders University for use in a research project.

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

The exemption will permit the use and disclosure of personal information for the purposes of a research project that will examine the Information Sharing practices of the OMP Pilot Program. The research project will be carried out under the supervision of the South Australia Police and Flinders University.

All other Principles continue to apply.

Conditions

This exemption is conditional on:

- the research project operating in accordance with the Offender Management Plan Information Sharing Protocol. It is subject to participating offenders being informed of the use of their information for the research project of the Offender Management Plan Pilot Program.
- the approval of the evaluation by a Human Research Ethics Committee constituted and acting in compliance with the *National Statement on Ethical Conduct in Human Research*.
- South Australia Police ensuring that no personal information that would identify an individual offender or from which an offender would be reasonably identifiable will be disclosed to a third party, other than the appointed researcher, as a result of the research project or any publications associated with the research project.

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 or until the end of the research project whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

12 December 2011

APPENDIX D Exemption Granted – Crime and social disorder in SA Housing Trust properties

Exemption – SAPOL & Housing SA (DFC)

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 personal 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:
    - 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;

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

- 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 three years from the date of its approval on 19 October 2011 or at the cessation of the Ministerial Agreement, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

26 October 2011

APPENDIX E Exemption Granted – SA NT DataLink

Exemption – Housing SA Dataset - DCSI

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 Housing SA, a business unit within the Department for Communities and Social Inclusion. It is an exemption from compliance with Principle 10, permitting Housing SA to disclose personal information to SA NT DataLink.

The personal information to be disclosed is from the Housing SA Dataset and is limited to:

- Unique Person Identifier
- System Date
- Names, all names including nicknames, aliases and aka
- Date of Birth
- Sex
- Title
- Aboriginality and/or Torres Strait Islander identifier
- Country of Birth
- Full address including geocodes if available
- Any of the above information provided for other family members and included in these records.

The information is to be disclosed for the purposes of the creation of master linkage keys as part of the establishment of the Data Linkage System by officers of the Department of Health (Health) within SA NT DataLink.

All other Principles continue to apply.

Conditions

The information disclosed 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 disclosed to, and accessed by, officers of Health.

Housing SA 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*.

---

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

Expiry

This exemption will be reviewed by Housing SA, SA NT DataLink 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

27 October 2011

Exemption – Housing SA Dataset - Department of Health

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 Department of Health (Health). It is an exemption from compliance with Principle 8, permitting Health to use personal information for a purpose other than the purpose for which it was collected.

The personal information to be used is from the Housing SA Dataset and is limited to:

- Unique Person Identifier
- System Date
- Names, all names including nicknames, aliases and aka
- Date of Birth
- Sex
- Title
- Aboriginality and/or Torres Strait Islander identifier
- Country of Birth
- Full address including geocodes if 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 Health located within SA NT DataLink.

All other Principles continue to apply.

Conditions

The information disclosed 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 disclosed to, and accessed by, officers of Health.

---

[9] *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 will be reviewed by Health, SA NT DataLink 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

27 October 2011

APPENDIX F Exemption Granted – OCSAR Evaluation – South Australian Aboriginal Courts and Conferences

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[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 Department of Justice. It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information in the conduct of a study into re-offending following sentencing in South Australian Aboriginal Courts and Conferences. The personal information to be collected and used in the study will include information from South Australia Police offence data, court records and Department of Correctional Services records of time spent in custody.

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

- Name, date of birth and sex
- Court attendance records
- Court outcome imposed
- Time spent in custody; and
- Number of offences and most serious offence (based on major charge) prior to and following participation in a Court/Conference (or mainstream court for relevant control groups).

The purpose of collection and use is to allow OCSAR to undertake a study of South Australian Aboriginal Courts and Conferences.

All other Principles continue to apply.

Conditions

This exemption is subject to the project receiving approval from a South Australian Government Human Research Ethics Committee constituted and operating in accordance with the *National Statement on Ethical Conduct in Human Research*.

The exemption is also conditional on OCSAR ensuring that no personal information that would identify an individual offender or from which an offender would be reasonably identifiable will be disclosed to a third party, other than the appointed researcher, as a result of the research project or any publications associated with the research project.

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).

[10] *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 is provided until 30 June 2012. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

12 December 2011

APPENDIX G Exemption Granted – Health Consumer

Exemption – Department of Health

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 applies to the Department of Health and incorporated hospitals and health centres (inclusively, the Department), exempting them from complying with Information Privacy Principle (IPP) 2. This exemption allows the collection of health information from a health consumer, or from a person responsible[12] for the health consumer, about a third party without the consent of the third party in circumstances where:

- the collection of the third party's information into a consumer's social, family or medical history is necessary for the Department to provide a health service directly to the consumer; and
- the third party's information is relevant to the family, social or medical history of that consumer; and
- the third party's information is only collected from a person responsible for the health consumer if the health consumer is physically or legally incapable of providing the information themselves.

IPP 2 will continue to apply outside of the conditions of this exemption. Health service providers that collect third party information into social, family or medical histories will still need to comply with the protections afforded under IPPs 4, 7, 8, 9 and 10 regarding the storage, use and disclosure of the information for the purpose for which it was collected.

The conditions of this exemption are similar to the Public Interest Determinations (PIDs) 12 and 12A granted by the Australian Privacy Commissioner under the operation of the *Privacy Act 1988 (Cth)* (effective 11 December 2011).

The PIDs have been issued for a period of 5 years. This exemption will expire at the same time as the expiry of PIDs 12 and 12A being the 10 December 2016, or earlier by review.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

17 January 2012

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

[12] For the purposes of this exemption a 'person responsible' has the same meaning as defined in Principle 2.5 of the *Code of Fair Information Practice.*

Exemption – Department of Communities and Social Inclusion

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[13] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This applies to the Department of Communities and Social Inclusion and incorporated hospitals and health centres (inclusively, the Department), exempting them from complying with Information Privacy Principle (IPP) 2. This exemption allows the collection of health information from a health consumer, or from a person responsible[14] for the health consumer, about a third party without the consent of the third party in circumstances where:

- the collection of the third party's information into a consumer's social, family or medical history is necessary for the Department to provide a health service directly to the consumer; and
- the third party's information is relevant to the family, social or medical history of that consumer; and
- the third party's information is only collected from a person responsible for the health consumer if the health consumer is physically or legally incapable of providing the information themselves.

IPP 2 will continue to apply outside of the conditions of this exemption. Health service providers that collect third party information into social, family or medical histories will still need to comply with the protections afforded under IPPs 4, 7, 8, 9 and 10 regarding the storage, use and disclosure of the information for the purpose for which it was collected.

The conditions of this exemption are similar to the Public Interest Determinations (PIDs) 12 and 12A granted by the Australian Privacy Commissioner under the operation of the *Privacy Act 1988 (Cth)* (effective 11 December 2011).

The PIDs have been issued for a period of 5 years. This exemption will expire at the same time as the expiry of PIDs 12 and 12A being the 10 December 2016, or earlier by review.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

17 January 2012

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

[14] For the purposes of this exemption a 'person responsible' has the same meaning as defined in Principle 2.5 of the *Code of Fair Information Practice.*

APPENDIX H Exemption Granted – SA NT DataLink

Exemption – Families SA Dataset - DECD

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[15] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Education and Child Development (DECD). It is an exemption from compliance with Principle 10, permitting DECD to disclose personal information to the Data Linkage Unit within SA NT DataLink.

The personal information to be disclosed is from the Families SA Dataset, specifically to support the linkage with Families SA data on Alternative Care, Care and Protection Orders, and Child Protection, and is limited to:

- Record identifier
- Names – all names including nicknames, aliases and aka
- Date of birth
- Sex
- Aboriginality, Torres Strait Islander indicator
- Cultural Group
- Full address including geocodes where available
- Client File Number (85 File Number for Client Information System (CIS) records within the Justice Information System (JIS) – a flag indicating that this child was under the Guardianship of the Minister)
- Any of the above information provided for other family members and included in these records, ie full name and date of birth of the mother and father of the child or young person.

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the further development 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 DHA within the Data Linkage Unit.

DECD remains responsible for the secure transfer 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*.

---

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

Expiry

This exemption is granted from 14 March 2012 to 11 December 2015. It will be reviewed by DECD 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

Exemption – Families SA Dataset - DHA

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[16] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Health and Ageing (DHA). It is an exemption from compliance with Principle 8, allowing DHA to use personal information for a purpose that was not the purpose of the collection of that information.

The personal information to be used is from the Families SA Dataset, specifically to support the linkage with Families SA data on Alternative Care, Care and Protection Orders, and Child Protection, and is limited to:

- Record identifier
- Names – all names including nicknames, aliases and aka
- Date of birth
- Sex
- Aboriginality, Torres Strait Islander indicator
- Cultural group
- Full address including geocodes where available
- Client File Number (85 File Number for Client Information System (CIS) records within the Justice Information System (JIS) – a flag indicating that this child was under the Guardianship of the Minister)
- Any of the above information provided for other family members and included in these records, ie full name and date of birth of the mother and father of the child or young person.

All other Principles continue to apply.

---

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

Conditions

The information is only to be used for the creation of master linkage keys in the further development 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 DHA within the Data Linkage Unit.

DHA 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*.

Expiry

This exemption is granted from 14 March 2012 to 11 December 2015. It will be reviewed by DHA 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

Exemption – Public Schools Enrolment Dataset - DECD

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[17] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Education and Child Development (DECD). It is an exemption from compliance with Principle 10, allowing DECD to disclose personal information to the Data Linkage Unit within SA NT DataLink.

The personal information to be disclosed is from the DECD Public Schools Enrolment Dataset and is limited to:

- Record Identifier
- Personal Identifier
- Names
- Date of Birth
- Sex
- Aboriginality, Torres Strait Islander Indicator
- Country of Birth

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

- Full address including Geocodes if available
- Parent / Guardian Identifier
- Date Enrolled
- Date Left
- Destination School
- Census year
- Census term
- Any of the above information provided for other family members and included in these records including family code.
- 85 File Number

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the further development 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 DHA within the Data Linkage Unit.

DECD remains responsible for the secure transfer 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 is granted from 14 March 2012 to 11 December 2015. It will be reviewed by DECD 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

Exemption – Public Schools Enrolment Dataset - DHA

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[18] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Health and Ageing (DHA). It is an exemption from compliance with Principle 8, allowing DHA to use personal information for a purpose that was not the purpose of the collection of that information.

The personal information to be used is from the Department for Education and Child Development (DECD) Public Schools Enrolment Dataset and is limited to:

- Record Identifier
- Personal Identifier
- Names
- Date of Birth
- Sex
- Aboriginality, Torres Strait Islander Indicator
- Country of Birth
- Full address including Geocodes if available
- Parent / Guardian Identifier
- Date Enrolled
- Date Left
- Destination School
- Census year
- Census term
- Any of the above information provided for other family members and included in these records including family code.
- 85 File Number

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the further development 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 DHA within the Data Linkage Unit.

---

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

DHA 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 is granted from 14 March 2012 to 11 December 2015. It will be reviewed by DHA 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

Exemption – South Australian Cancer Registry Dataset - DHA

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[19] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Health and Ageing (DHA). It is an exemption from compliance with Principle 8, allowing DHA to use personal information for a purpose that was not the purpose of the collection of that information.

The personal information to be used is from DHA's South Australian Cancer Registry Dataset and is limited to:

- Personal Identifier
- Names – all names including nicknames, aliases and aka
- Date of birth
- Date of death
- 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.

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the further development 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 DHA within the Data Linkage Unit.

DHA 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 is granted from 14 March 2012 to 11 December 2015. It will be reviewed by DHA 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

Exemption – Public Hospital Inpatients Morbidity Dataset and Emergency Department Dataset - DHA

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[20] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Health and Ageing (DHA). It is an exemption from compliance with Principle 8, allowing DHA to use personal information for a purpose that was not the purpose of the collection of that information.

The personal information to be used is from DHA's Public Hospital Inpatients Morbidity Dataset and the Emergency Department Dataset and is limited to:

- Personal Information
  - Personal Identifier
  - Names – all names including nicknames, aliases and aka
  - Date of birth
  - Sex
  - Title
  - Aboriginality, Torres Strait Islander Indicator

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

- Country of birth
- Full address

- Event information
  - Dates of admission and discharge

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the further development of the master linkage file as part of the SA NT Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of DHA within the Data Linkage Unit.

DHA 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 is granted from 14 March 2012 to 11 December 2015. It will be reviewed by DHA 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

APPENDIX I Exemption Granted – Seniors Card / Adelaide Fare Collection System

Exemption – DHA

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[21] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Health and Ageing (DHA). It is an exemption from compliance with Principle 10, allowing DHA to disclose information collected during the application process of current Seniors Card holders to the Department of Planning, Transport and Infrastructure (DPTI) for inclusion in the Adelaide Fare Collection System (AFCS).

The personal information to be disclosed is:

- Seniors Card Number (7 digit unique number for all card holders)
- Title
- First Name
- Last Name
- Date of Birth
- Address Line 1
- Address Line 2
- Suburb
- State
- Postcode

The purpose of disclosure is to allow for the storage of Seniors Card holder's personal information in the AFCS in order to register Seniors Card holders in the AFCS and to provide Seniors Card holders with all levels of DPTI customer services, including telephone service.

All other Principles continue to apply.

Conditions

This exemption is a once only exemption for DHA to disclose the personal information of the current Senior Card holders to DPTI for the AFCS.

---

[21] *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 is a once only exemption and will expire after DHA have disclosed the personal information of Seniors Card holders to DPTI for inclusion in the AFCS.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

19 June 2012

Exemption – DPTI

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[22] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department of Planning, Transport and Infrastructure (DPTI). It is an exemption from compliance with Principles 2 and 8, allowing DPTI to collect information of current Seniors Card holders and use information collected during the application process of current Seniors Card holders by the Department for Health and Ageing for inclusion in the Adelaide Fare Collection System (AFCS).

The personal information to be collected and used is:

- Seniors Card Number (7 digit unique number for all card holders)
- Title
- First Name
- Last Name
- Date of Birth
- Address Line 1
- Address Line 2
- Suburb
- State
- Postcode

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

The purpose of collection and use is to allow DPTI to register and store Seniors Card holders personal information in the AFCS and to provide Seniors Card holders with all levels of DPTI customer services, including telephone service.

All other Principles continue to apply.

Conditions

The exemption from IPP2 will be a once only exemption to allow DPTI to collect the information disclosed by the Department for Health and Ageing collected during the application process of current Seniors Card holders.

The exemption from IPP8 is ongoing.

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 granted from 13 June 2012 to 13 June 2015. This exemption will be reviewed by DPTI 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 June 2012

APPENDIX J Exemption Granted – Intervention Orders and the Intervention Response Model

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[23] (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 South Australia Police (SAPOL) and the Courts Administration Authority (CAA) to allow OCSAR to undertake an evaluation of Intervention Orders and the Intervention Response Model.

The collection of personal information is required to enable OCSAR to match records held about applications to the Court for Intervention Orders, with SAPOL offending records, and is limited to:

- Family name
- Given name
- Address
- Ethnicity
- Date of birth
- Gender
- Information held on the Justice Information System (JIS), including:
  - Conditions of Intervention Orders issued
  - Amount and type of offending for 12 months pre-Intervention Order
  - Amount and type of offending for 12 months post-Intervention Order
  - Number of breaches of an Intervention Order
  - Type of conditions breached
  - Type of penalties received for breach of Orders; and
  - Whether the individual has participated in an Intervention Program as part of their Order.

All other Principles continue to apply.

Conditions

This exemption is conditional on OCSAR obtaining approval for the evaluation from the Families and Communities Research Ethics Committee.

Security of Personal Information

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

[23] *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 is provided for two years, for the period 27 June 2012 to 26 June 2014. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

24 July 2012

Exemption – CAA & SAPOL

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[24] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Courts Administration Authority (CAA) and the South Australia Police (SAPOL). It is an exemption from compliance with Principle 10, allowing CAA and SAPOL to disclose personal information to the Office of Crime Statistics and Research (OCSAR) to facilitate an evaluation by OCSAR of Intervention Orders and the Intervention Response Model.

The personal information to be disclosed is limited to:

- Family name
- Given name
- Address
- Ethnicity
- Date of birth
- Gender
- Information held on the Justice Information System (JIS), including:
    - Conditions of Intervention Orders issued
    - Amount and type of offending for 12 months pre-Intervention Order
    - Amount and type of offending for 12 months post-Intervention Order
    - Number of breaches of an Intervention Order
    - Type of conditions breached
    - Type of penalties received for breach of Orders; and
    - Whether the individual has participated in an Intervention Program as part of their Order.

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

All other Principles continue to apply.

Conditions

This exemption is conditional on OCSAR obtaining approval for the evaluation from the Families and Communities Research Ethics Committee.

Security of Personal Information

The security of the personal information must 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 two years, for the period 27 June 2012 to 26 June 2014. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

24 July 2012