Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2013

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 2013

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 John Rau MP
ATTORNEY-GENERAL

Dear Attorney-General

The Privacy Committee of South Australia is pleased to provide you with this report of its activities for the year ending 30 June 2013. The report is provided pursuant to Clause 4A of the *Proclamation establishing the Privacy Committee of South Australia*, as amended and republished in the South Australian Government Gazette on 11 June 2009.

Terry Ryan
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

30 September 2013

Table of Contents

1 Year in Review

It has been another challenging year for the Privacy Committee of South Australia with significant developments in privacy reform across Australia including changes to the State Government's administrative scheme for information privacy.

The Privacy Committee followed with interest the progress of reforms to the Commonwealth *Privacy Act 1988*. The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* passed through the Commonwealth Parliament in November 2012 to finalise the most significant changes to federal privacy legislation in twenty years. The changes will have an impact on all South Australians with the establishment of a new single set of privacy principles to apply to both private sector organisations and Commonwealth Government agencies. The amendments will also increase the accessibility of personal information for credit reporting purposes and provide greater enforcement powers for the Commonwealth Privacy Commissioner.

The significant changes at the Commonwealth level reinforce the need for reform of the State's administrative scheme for privacy. The Information Privacy Principles Instruction (IPPI) has not changed substantially since it was established over twenty years ago. South Australia remains one of only two Australia jurisdictions without legislation protecting personal information in its public sector.

The Privacy Committee is increasingly concerned about the ability of the IPPI to provide an adequate framework for protecting personal information in South Australian government agencies. The concerns have emerged in light of the increased focus of government on delivering services collaboratively and online, the further technological development in government information systems, such as the Department for Health and Ageing's proposed Electronic Patient Administration System, and the ongoing threat of cyber-crime in Australia. The IPPI was developed at a time when coordinated service provision in government was not the norm, information was primarily held in paper files and the internet in Australia was in its infancy.

Some of the Privacy Committee's concerns with the IPPI were highlighted in the final report of the Independent Education Inquiry undertaken by the Honourable Bruce Debelle AO QC. The final report of the Inquiry recommended changes to the disclosure provisions of the IPPI and highlighted the lack of effective compliance measures to support the IPPI. It also recommended changes to the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children Young People and their Families* to promote consistency with the recommended update to the IPPs.

The Privacy Committee supports the changes to the IPPs recommended by the Inquiry. The Committee believes the changes will strike an appropriate balance between the use and disclosure of personal information to prevent harm to individuals and the right to individual privacy. However further reform is also needed to support appropriate information sharing in the public sector.

The Privacy Committee supports the development of information privacy legislation for the South Australian public sector to address these challenges. Legislation would ensure the personal information of South Australian citizens that is held by the public sector is afforded privacy protections consistent with that in other Australian states and territories, and provide a framework for the appropriate sharing of personal information. It would promote greater awareness of, and improve compliance with, the IPPs.

In addition to these important developments, the Privacy Committee continued to provide advice and recommendations to the Minister and government agencies on the protection of privacy and the IPPI. It also continued to fulfil its role in receiving privacy complaints, responding to privacy enquiries and granting exemptions from the IPPs that it considered in the public interest. During the reporting year, the Privacy Committee extended or granted seven exemptions from the IPPs to State Government agencies (see item 3.7), concluded one complaint (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 159 enquiries from the public and State Government agencies, which is moderately higher than the number of enquiries handled in the previous year (see item 2.2.4).

This is a report of the activities of the Privacy Committee for the year ending 30 June 2013. 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 Instruction

South Australia's Information Privacy Principles Instruction (IPPI) was introduced in July 1989 by means of *Cabinet Administrative Instruction 1/89*, issued as *Premier & Cabinet Circular No. 12*, and is more commonly known as the Information Privacy Principles (IPPs). The IPPs regulate the way South Australian Public Sector agencies collect, use, store and disclose personal information.

The IPPs were amended in February 2013 as a result of work undertaken by the Interagency Task Force for the Disclosure of Sexual Offences. The Task Force was established to coordinate the Government's response to the issues considered by the Independent Education Inquiry (see also 3.3.10).

IPP 10 was amended to permit an agency to disclose personal information where the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

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 and imminent threat to the life or health of someone;
- it is required by law;
- it is required for enforcing a law, protecting public revenue, or protecting the interests of the government as an employer; or

- where the agency has reason to suspect unlawful activity has been, is being or may be engaged in.

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 and imminent 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 IPPI 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 IPPI on the State Records website, and in Appendix B of this report.

2.2.2 Reporting

During 2012-13, the Privacy Committee reported initially to the Hon Michael O'Brien MP, Minister for the Public Sector and, from February 2013, to the Hon John Rau MP, Deputy Premier and Attorney-General.

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 responsible for the administration of the *Health Care Act 2008*
- 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:

- Deslie Billich, non-public sector employee (commenced December 2012)
- Tanya Hosch, non-public sector employee (resigned August 2012)
- 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, A/Director, Business Affairs, Department for Communities and Social Inclusion
- Andrew Stanley, nominee of the Minister for Health.

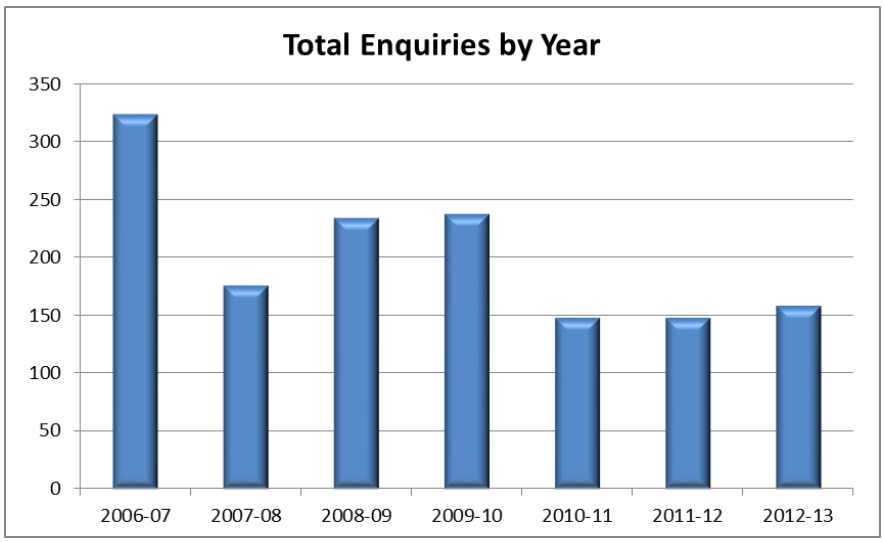
The term of appointment for each of the current members expires on 5 December 2014, with the exception of Ms Billich, whose appointment expires on 30 September 2014.

2.2.4 Resources

State Records of South Australia (State Records) provides executive support to the Privacy Committee including research and policy support, administrative support, meeting coordination, web hosting, and an enquiry and advice service to both agencies and the public. This resource includes the commitment of approximately 1.2 full time equivalents.

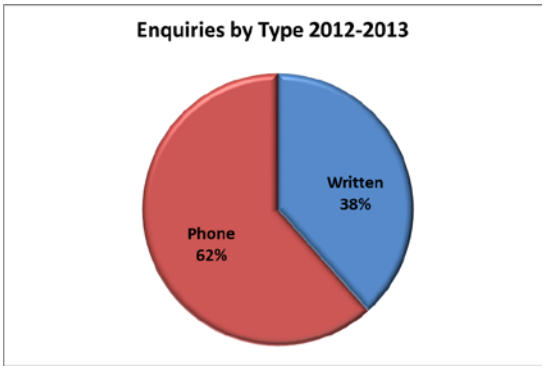
2.2.4.1 Privacy Enquiries

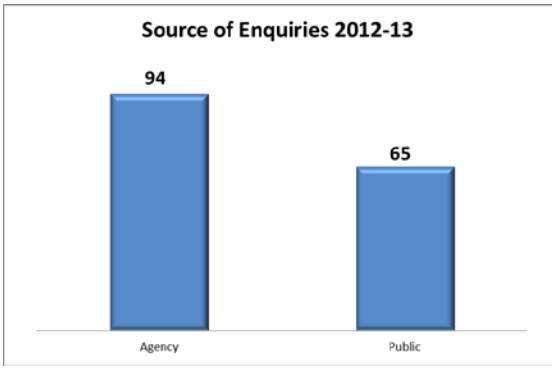
During the reporting year, State Records responded to 159 telephone and email enquiries from the public and State Government agencies relating to all aspects of privacy of personal information. This is seven per cent higher than the number of enquiries reported in the previous reporting year.



Over the reporting year 62% of all enquiries were dealt with over the telephone. The number of enquiries received from the public decreased by 29% from 92 reported last year to 65 reported for 2012-13. The number of enquiries received from State Government agencies increased by 68%, from 56 reported last year to 94 for 2012-13.

Overall, 60% of all enquiries received were from State Government agencies.





2.2.4.2 Privacy Training

State Records conducted one 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 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 Premier and Cabinet Circulars | dpc.sa.gov.au.

Members of the Privacy Committee that are not public sector employees are entitled to sessional fees. Payments for sessional fees for the Privacy Committee during 2012-13 totalled $206.

2.2.6 Meetings

During the reporting year the Privacy Committee met on seven occasions. Where necessary meetings were supplemented by the conduct of business out of session.

2.2.7 Guidelines for members

A handbook for members contains information on the role of the Privacy Committee, its relationship to other approval and advisory bodies, duties and obligations of members, the process for handling complaints, and other information of value to members in performing their role. It also includes a brief history of privacy law and self-regulation in South Australia, and an overview of the protection of personal information in other Australian jurisdictions.

The handbook was updated in January 2013.

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 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 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.

The constitution of the Privacy Committee meets 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.

2.2.9 Seven Strategic Priorities

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 and 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 supports the implementation of the priorities in relation to safe communities, healthy neighbourhoods and every chance for every child, in particular through its endorsement of the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families*, its provision of exemptions for the Offender Management Plan, SA NT DataLink and the Way2Go Program.

3 Activities of the Privacy Committee

3.1 Advice to the Minister

Under clause 2(a) of the Proclamation, the Privacy Committee has the function *'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 privacy reform in South Australia, amendments to the IPPs, the Australian Early Development Index, and the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children Young, People and their Families*.

During the year 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 support the project to develop the legislation. The Committee remains concerned about the absence of a legislative framework for information privacy in the South Australian public sector.

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 with the exception of Western Australia. 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 achieved in national privacy law reform during the year with the passing of substantial amendments to the Commonwealth *Privacy Act 1988* (Privacy Act). On 29 November 2012, the Australian Parliament passed the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Act). The Act received Royal Assent on 12 December 2012. The Act was the latest development in the Australian Government's response to the Australian Law Reform Commission's (ALRC) *Report 108* on Australian privacy law and practice.

The Privacy Act was amended to achieve three key reforms. The first was the establishment of the Australian Privacy Principles (APPs) that replace the two existing sets of privacy principles. The APPs will guide the handling of personal information in both Commonwealth Government agencies and private sector organisations. The second was the revision of the credit reporting provisions to 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 was to increase the powers of the Commonwealth Privacy Commissioner to enforce the Privacy Act. These amendments will come into force on 12 March 2014.

3.2.1.3 National Electronic Health Reform

The Australian Government continued to progress national electronic health reform in 2012-13 through the implementation of the Personally Controlled Electronic Health Records (PCEHR) system.

The PCEHR system will provide individuals the opportunity to access their health information when and where they need it and to share this information with relevant healthcare providers. Healthcare providers see its potential in improved communication of clinical information between healthcare professionals to provide more comprehensive and quality healthcare services. This includes the potential for more efficient and accurate transfer of health information across the health sector.

In July 2012, the PCEHR System started taking registrations from individuals for an eHealth Record. The Office of the Australian Information Commissioner

(OAIC) released a range of resources to assist the public to understand how privacy issues were managed under the PCEHR system.

During the reporting year, the Privacy Committee participated in further discussions with the OAIC and other State and Territory privacy and health regulators in the establishment of a privacy complaints handling framework for the PCEHR system. The Information Sharing and Complaints Referral Agreement for the PCEHR was finalised and published by the OAIC in June 2013. The Privacy Committee is not party to the agreement but has informally agreed to refer any relevant complaints in line with the agreement. The Privacy Committee noted that the South Australian Health and Community Services Complaints Commissioner joined as a party to the agreement in June 2013.

The Committee will continue to keep itself informed of the implementation of the PCEHR system as it progresses in 2013-14.

3.2.1.4 National Heavy Vehicle Regulation

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

The NHVL is being developed with the aim of reducing red tape and improving productivity and safety in the heavy vehicle industry. The law will be administered by the new National Heavy Vehicle Regulator. It will apply to all vehicles over 4.5 tonnes and is expected to come into effect in South Australia in late 2013.

During the reporting year, the Privacy Committee provided further advice to the Department of Planning, Transport and Infrastructure on the information privacy arrangements to be established under the NHVL to support the State's response to national consultations.

The *Heavy Vehicle National Law (South Australia) Bill 2013* was introduced to the South Australian Parliament on 2 May 2013. Under the Bill, the Queensland *Information Privacy Act 2009* will apply to the new National Heavy Vehicle Regulator. However, where a state or territory authority is undertaking functions under the national law that respective state or territory's information privacy regime will apply.

3.2.1.5 National Rail Safety Regulator

In June 2012, the *Rail Safety National Law (South Australia) Act 2012* (RSNL) was passed by the South Australian Parliament. The RSNL has been adopted by a number of other Australian States and Territories and will eventually create a single scheme for rail safety oversight across Australia to replace existing State and Territory based regulation. The RSNL established the National Rail Safety Regulator to provide oversight of rail safety in participating jurisdictions. South Australia was selected as the host jurisdiction for the Regulator. The Regulator commenced operations on 20 January 2013 with oversight of rail safety in South Australia, New South Wales, Tasmania and Northern Territory. Oversight of the other Australian States and Territories is expected to commence in the second half of 2013.

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 South Australian 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 law in South Australia prevented the immediate adoption of a similar approach for privacy oversight. The lack of any formal information privacy oversight covering the Regulator remains of concern to the Committee, particularly given the types of sensitive personal information the Regulator will collect.

3.2.1.6 Statutory Cause of Action for Invasion of Privacy

On 12 June 2013, the Commonwealth Attorney-General Mark Dreyfus QC asked the ALRC to conduct an inquiry into the protection of privacy in the digital era. The inquiry will address both prevention and remedies for serious invasions of privacy. This builds on the previous work of the ALRC and the Commonwealth Government on the establishment of a Statutory Cause of Action (a right to sue) for Invasion of Privacy. The ALRC is to report to the Attorney-General by June 2014.

The Privacy Committee has previously supported a recommendation of the ALRC for the establishment of a Statutory Cause of Action for Invasion of Privacy. The Committee also made a submission to the Commonwealth Government's consultation on a Statutory Cause of Action.

In addition, the Committee became aware that the South Australian Law Reform Institute was considering a review of the need for a South Australian tort of law for invasion of privacy.

The Privacy Committee will keep itself informed of both the work of the latest inquiry of the ALRC and that of the SA Law Reform Institute during 2013-14.

3.2.1.7 Victorian Privacy and Information Security Reforms

In December 2012, the Victorian Government announced a major reform to its privacy regime. The Government announced its intention to establish a new Privacy and Data Protection Commissioner. This reform aims to bring together privacy and data security by overtly linking the legal obligation to keep personal information secure under the Victorian *Information Privacy Act 2000* with a new set of data security standards. The establishment of the Commissioner will bring together the existing offices of the Privacy Commissioner and the Commissioner for Law Enforcement Data Security.

The Privacy Committee will continue to keep itself informed on the reform as it progresses in 2013-14.

3.2.1.8 Privacy Amendment (Privacy Alerts) Bill 2013

On 29 May 2013 the Commonwealth Government introduced the *Privacy Amendment (Privacy Alerts) Bill 2013* into the Australian Parliament. The

Bill seeks to amend the *Privacy Act 1988* to provide for the mandatory disclosure of data breaches involving personal information. The Bill provides for individuals affected by data breaches to be notified where there is a real risk of serious harm to the individuals arising from the breach.

The Bill was referred to the Senate Standing Committee on Legal and Constitutional Affairs on 18 June 2013. The Senate Committee wrote to the Privacy Committee inviting comment on the Bill. The Privacy Committee was not able to respond to the consultation due to the short timeframe available for a response.

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 Privacy Authorities of Australia (PAA).

3.2.2.1 Asia Pacific Privacy Authorities

Asia Pacific Privacy Authorities (APPA), formed in 1992, is the principal forum for privacy authorities in the Asia Pacific Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints.

A representative of the Privacy Committee usually attends at least one meeting of APPA during each financial year. The Committee has observer status at APPA. Due to budget constraints the Committee was not represented at a meeting of APPA in 2012-13.

However, the Privacy Committee continued to keep itself informed of developments at APPA during the year including the work of the APPA Technology Working Group.

Key issues considered by APPA during 2012-13 included:

- Data breach notification laws
- Global privacy enforcement
- Privacy Awareness Week
- Google's privacy policy changes
- Cross-border privacy rules.

Further information about APPA can be found at http://www.appaforum.org/.

3.2.2.2 Privacy Authorities of Australia (PAA)

The Privacy Committee was represented at a meeting of the PAA via teleconference on 7 May 2013.

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 Privacy Committee with an opportunity to connect with other Australian privacy authorities and keep itself informed about developments in other jurisdictions.

The meeting in May considered privacy issues in relation to:

- National and State privacy law reforms
- National regulatory schemes
- Cross sector data linkage
- Big Data
- E-health
- Australian Early Development Index
- Document Verification Service.

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 during the reporting year. Key instances are described below.

3.3.1 Adelaide Fare Collection System (MetroCard and Seniors Card)

The Adelaide Fare Collection System (AFCS) is the IT system that supports South Australia's transport smartcard, MetroCard. The MetroCard was introduced by the Government across the State's public transport network in November 2012. The introduction of the MetroCard was complemented by the introduction of a new Seniors Card that incorporates the MetroCard technology.

In February 2013, following an enquiry from a member of the public, the Privacy Committee reviewed the exemptions provided to Department for Health and Ageing (DHA) and Department of Planning, Transport, and Infrastructure (DPTI) in the previous financial year in relation to the new Seniors Card. The exemptions provided were to permit the disclosure of personal information by DHA to the DPTI for inclusion in the Adelaide Fare Collection System to enable the issuing of the new Seniors Card. The Privacy Committee was concerned that seniors card holders were not provided with adequate information about the implications of the new card and about their options to travel anonymously on public transport.

The Privacy Committee wrote to DHA and DPTI about this matter in March 2013. DHA responded in May 2013 and advised that the agencies were working closely to improve the information available to seniors card holders about how they might de-identify their customer record to allow anonymous travel and about the information disclosed by DHA to DPTI.

3.3.2 SA NT DataLink

SA NT DataLink is an unincorporated joint venture, comprising South Australian and Northern Territory Government and non-government organisations.
SA NT DataLink enables the linkage of administrative and clinical datasets to allow population level health, social, education and economic research and evidence-based policy development to be undertaken with de-identified data,

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 through the granting of a number of exemptions. The exemptions allow State Government agencies to disclose limited identifying variables, such as name, date of birth and address, to SA NT DataLink for inclusion in its Master Linkage File (MLF) to enable the creation of links between multiple government datasets. The exemptions are subject to strict conditions on the governance of data, including approval from a South Australian Government Human Research Ethics Committee (HREC) for each research project enabled by SA NT DataLink.

The Privacy Committee continued to work with SA NT DataLink in 2012-13 to ensure appropriate governance in the maintenance and development of the MLF. Of particular interest in 2012-13, the Privacy Committee granted exemptions from the IPPs to permit the addition of identifying variables from the South Australian Electoral Roll dataset to the MLF. In providing these exemptions the Privacy Committee deemed that there was significant public interest in doing so given the potential research that would be enabled through data linkage using these datasets.

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

(See 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.

The Privacy Committee is represented on the South Australian Identity Security Management Group. The group supports cross agency information sharing on identity security matters and assists the Government to respond to national identity issues.

In 2012-13 the Privacy Committee continued to provide advice to the Government to support an update of the National Identity Security Strategy (NISS). The purpose of the NISS is to guide a national approach to ensure Australians are able to confidently enjoy the benefits of a secure and protected identity.

The revised NISS was released by the Council of Australian Governments in December 2012.

During the year, the Committee provided advice to support the State's response to the development of a number of NISS projects including the:

- expansion of the Document Verification Service to the private sector; and
- National Biometric Interoperability Framework.

3.3.6 Australian Early Development Index

The Australian Early Development Index (AEDI) is a national progress measure for the National Early Childhood Development Strategy, an initiative of the Council of Australian Governments. AEDI is also a key target (T 12) of South Australia's Strategic Plan.

AEDI involves the collection of information to help create a snapshot of children's development in communities across Australia every three years. The collection requires teachers to complete a survey for each child in their first year of full-time school. The survey measures the following 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.

In its 2011-12 Annual Report the Privacy Committee noted that it had received a submission from the Department for Education and Child Development (DECD) seeking an 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 AEDI survey. 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 to fulfil the primary purpose of the survey and that no identified data should be collected. Despite the Committee's concerns, the personal information was disclosed to the Commonwealth to facilitate the 2012 AEDI collection. The Committee considered this a breach of the IPPI.

The Privacy Committee's concerns with the disclosure related to 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 purpose of pre-population of the AEDI survey DECD would require informed consent. The letter DECD provided to parents to inform them of the collection provided an option to opt-out of the collection. The Committee did not consider this process gave parents adequate opportunity to provide informed consent. The Committee was also concerned that parents were not provided sufficient information about the future storage and use of the information collected by the Commonwealth. The Privacy Committee is committed to continuing to work through its concerns with DECD and DEEWR prior to the next AEDI collection scheduled for 2015.

3.3.7 Summary Offences Act – Filming Offences

During the year, the Privacy Committee provided comments to the Attorney-General's Department on amendments to the *Summary Offences Act 1953* in relation to filming offences. The Privacy Committee broadly supported the amendments.

The amendments created new offences to prevent humiliating and degrading filming and the uploading of the product of such filming to the internet and restated existing indecent filming offences. The amendments also made it an offence to distribute invasive images. This offence aims to prevent the uploading of images of a private and intimate nature on the Internet without the consent of the subject of the image. The *Summary Offences (Filming Offences) Amendment Bill 201*2 was passed by Parliament and received assent on 14 March 2013. The amendments are due to come into force on 1 July 2013.

3.3.8 Independent Education Inquiry

The Privacy Committee noted the Government's announcement on 1 November 2012 of the Independent Education Inquiry (Inquiry) to be conducted by former Supreme Court Justice, the Honourable Bruce Debelle AO QC. The Inquiry was to consider a particular case concerning DECD's failure to disclose information to parents about a child sexual assault in a South Australian public school. In late 2012, the Inquiry was provided with the powers of a Royal Commission. The Inquiry Report was presented to the Government on 21 June 2013.

As part of its response to the issues considered by the Inquiry, the Government amended the IPPs on 4 February 2013 to include a new disclosure clause 4(10)(f) to permit the disclosure of personal information by an agency where "the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities".

The Inquiry Report included a recommendation for a further amendment to the IPPs. The Report recommended that the existing IPP 4(10)(b) be amended to remove the term 'and imminent' and include the term 'or safety' that would provide for disclosure of personal information where:

> *the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or some other person*.

The Report also recommended the extension of the IPPI to cover the Governing Councils of schools.

The Privacy Committee also noted the Inquiry's observation that, apart from any public disapproval that might follow from the tabling of the Privacy Committee's Annual Report in Parliament, there is no effective sanction to ensure compliance with the IPPI. The Committee agrees with the observation of the Inquiry and supports the establishment of information privacy legislation in South Australia to replace the IPPI to promote agency compliance with information privacy protections.

The Privacy Committee is committed to working with the Government in 2013-14 to implement the recommendations of the Inquiry as they relate to the IPPI and to promote further improvement in information sharing by Government agencies to protect children from harm.

3.3.9 Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families

The *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families* (ISG) were established in 2008 to promote appropriate and timely sharing of information to lessen or prevent risks to the safety and wellbeing of children, young people and their families. The ISG promotes early intervention and service coordination to prevent harm, and encourages information sharing with the consent of the person to whom the information relates where it is safe and reasonable in the circumstances. Where it is not safe or reasonable to seek consent, the ISG provides a framework for appropriate information sharing without consent.

During the year, the Privacy Committee was consulted on a proposal to extend the application of the ISG to address risks of harm to vulnerable adults. The Committee gave its in-principle support for the proposal to extend the application of the ISG. It recognised that the benefits of early intervention and service coordination to prevent serious risks to health, safety and wellbeing were not limited to children, young people and their families but equally applied in relation to vulnerable adults.

The Privacy Committee also noted that responsibility for the promotion of the ISG in State Government agencies was transferred from the Office of the Guardian for Children and Young People to the South Australian Ombudsman in March 2013 to reflect the intended broadening of the scope of the ISG.

Agencies observing the ISG are subject to an exemption from IPP 10(b), which has the intent of removing the words 'and imminent'. On 26 June 2013, the Privacy Committee granted a temporary exemption from the IPPs for the ISG, backdated from 6 April 2013 and expiring 18 September 2013 (see also item 3.7.6).

Should the Government adopt Independent Education Inquiry's recommended amendment to IPP 10(b), the ISG would not require an ongoing exemption from the IPPs (see 3.3.8).

3.3.10 Surveillance Devices Bill 2012

The *Surveillance Devices Bill 2012* was introduced into the South Australian Parliament on 5 September 2012. The Bill seeks to establish a new law to regulate the use of surveillance devices in South Australia to replace the existing *Listening and Surveillance Devices Act 1972* (LSDA). The Bill seeks to regulate a larger range of surveillance devices than the LSDA including tracking devices and data surveillance devices and to provide for cross-border recognition of warrants for the use of surveillance devices for law enforcement purposes.

The Bill passed through the House of Assembly in September 2012. On 21 February 2013, the Legislative Council referred the Bill to the Legislative Review Committee (LRC) for inquiry to consider:

- the need to protect a person's privacy from the use of surveillance devices against the person without consent;

- the circumstances in which persons should have the right to protect their lawful interest through the use of surveillance devices against another person without that person's consent;
- the circumstances in which it may be in the public interest for persons to use a surveillance device against another person without that person's consent; and
- the circumstances in which the communication or publication of information or material derived from the covert use of a surveillance device should be permitted.

The LRC invited the Privacy Committee to make a submission to the Inquiry in April 2013. The Privacy Committee provided its submission on 29 April 2013. The Privacy Committee broadly supported the Government's introduction of the Bill. It noted that the Bill addresses a gap in the provisions of the current LSDA by regulating a broader range of listening and surveillance devices, including provisions for tracking and data surveillance devices. It stated that new provisions covering these devices are important and necessary for improving privacy protection in South Australia.

The LRC Inquiry had not reported its findings before the end of the reporting year. The Privacy Committee will keep itself informed of the progress of the Bill in 2013-14.

3.4 To make publicly available, information as to methods of protecting individual privacy

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'*.

The limited resources available to support the Privacy Committee do not allow it to regularly make public statements or publish public guidance on existing or emerging threats to individual privacy. Its focus in this area is to participate where possible in State, National and International forums focussed on promoting the protection of privacy, such as the Privacy Authorities of Australia (see also item 3.2.3.1) and the Asia Pacific Privacy Authorities Forum (see also item 3.2.3.2). The Privacy Committee will continue to look at ways it can improve its performance of this function in 2013-14 within its limited resources.

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 to promote the protection of individual privacy. This includes representation on:

- the South Australian Government's ICT Security and Risk Steering Committee.
- 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 IPPs.

3.5.1 Privacy Breaches

3.5.1.1 Families SA

In its Annual Report for 2011-12, the Privacy Committee highlighted a breach of the IPPs which involved a confidential Families SA file being left in a filing cabinet that was subsequently sold at auction. The Privacy Committee indicated in its Annual Report that it would seek an update on Families SA's compliance with the IPPs during 2012-13.

In August 2012, the Privacy Committee was advised that a number of records management policies and procedures had been developed or updated as a result of the breach. It also noted that Families SA was utilising the DECD Information Management Policy – Privacy and Confidentiality and that this policy was to be reviewed by DECD in early 2013.

3.5.1.2 WorkCover Corporation of South Australia

In August 2012, the Privacy Committee noted media reports concerning the inadvertent disclosure of personal information by a contractor of WorkCover to a third party. The personal information of up to four WorkCover clients was inadvertently made to another client when they requested their own information under the *Freedom of Information Act 1991*. The information included confidential information relating to the injuries, health plans and medications of the clients.

The Privacy Committee notes that the WorkCover Corporation and its contractors are exempt from compliance with the IPPI. As a result the Committee had no power to investigate the breach of personal information by WorkCover. The Privacy Committee also notes that a private sector organisation is not bound by the Commonwealth *Privacy Act 1988* when contracted to provide services on behalf of a state or territory authority and, therefore, the Commonwealth Privacy Commissioner also had no power to investigate the breach by WorkCover's contractor. The Privacy Committee is concerned about this gap in the regulation of personal information in South Australia.

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 Committee will then 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 Committee may also refer the complainant to the South Australian Ombudsman if it remains 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 Ombudsman.

The Privacy 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 organisations to resolve privacy complaints and improve their practices when handling personal information.

During the reporting year there were two formal complaints received, with one complaint concluded and the other still ongoing at the end of 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	Public Health Service	IPP 10 – Disclosure of personal information to third party	Withdrawn
2	Government Department	IPP 10 – Disclosure of personal information to third party	Ongoing

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, such as an expiry date, an approval from an appropriate

research ethics committee or a requirement for the agency to report on the activity conducted under the exemption.

The Privacy Committee reviewed and updated the template used by agencies to request an exemption from the IPPs during the reporting year. The template was updated to improve the information provided to the Committee and to highlight the need for an agency to ensure all other necessary approvals have been obtained in order for the Committee to undertake an informed assessment of the proposal for consideration of an exemption.

Following is a summary of each request for exemption.

3.7.1 Post Event Patron Listings - BASS

In August 2012, the Privacy Committee considered and later granted an exemption from IPP 10 to the Adelaide Festival Centre Trust (AFCT). The exemption was a once only exemption to allow the AFCT's ticketing company BASS to disclose event specific patron listings to publically funded arts companies that perform in Adelaide Festival Centre venues. The disclosure was to enable the arts companies to contact their patrons to verify the patron's email and contact preferences.

See APPENDIX C for the full text of the exemption.

3.7.2 Community Protection Panel Alcohol and Other Drug Service Model

In 2010, the Privacy Committee granted an exemption from the IPPs to the Office of Crime Statistics and Research (OCSAR) to enable it to conduct a process evaluation of the Community Protection Panel (CPP). This exemption expired on 8 April 2012.

In October 2012, the Privacy Committee considered a further request by OCSAR for an exemption from IPPs 2 and 8 to permit the evaluation of the Alcohol and Other Drug (AOD) Service Model component of the CPP, which did not occur in the previous evaluation. The Committee approved the exemption to 30 June 2013. The exemption was conditional on the evaluation receiving approval from the Families and Communities Research Ethics Committee (FCREC) and the Aboriginal Health Research and Ethics Committee (AHREC).

The Privacy Committee was later made aware that the FCREC had deferred approval and requested further information from OCSAR. Consequently, OCSAR was advised that the exemption from the IPPs was not valid until such time as approval had been obtained from the FCREC. At the end of the reporting year, the Privacy Committee was advised that OCSAR would not be utilising the exemption.

See APPENDIX D for the full text of the exemption.

3.7.3 Offender Management Plan Pilot Program

In March 2010, an initial exemption was granted by the Privacy Committee to allow for information sharing between selected agencies in relation to the Offender Management Plan (OMP) pilot program in the Port Adelaide region. The agencies were South Australia Police (SAPOL), Department for Correctional Services (DCS), the then Department for Families and Communities (now

Department for Communities and Social Inclusion - DCSI), Attorney General's Department (AGD) and the then Department of Health (now Department for Health and Ageing - DHA).

The purpose of the OMP 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.

In November 2012, the Committee granted a further exemption up to June 2013 that also approved an amendment to include the personal information of family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender.

In April 2013, the Privacy Committee approved a further amendment to the exemption to include TAFE SA as a participating agency in the OMP pilot program. Due to machinery of government changes, TAFE SA was no longer part of DFEEST, and had been established as a State Government owned statutory authority.

In June 2013, the Privacy Committee considered and approved a further two year extension to the exemption for SAPOL, DCS, DCSI, DHA, AGD, DFEEST and TAFE SA to share case file information of serious offenders as part of the OMP pilot program. This 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. It is also conditional on the Pilot Practice Guidelines for the pilot program being finalised.

The Privacy Committee notes that the pilot program received a National Meritorious Police Award in November 2012. In addition, the August 2012 evaluation reports for pilot program showed improved rehabilitation prospects, health prospects, community safety, and a 52% reduction in overall offending.

See for the full text of the exemptions.

3.7.4 Way2Go Program

In December 2008, the Privacy Committee considered a request from the then Department of Transport, Energy and Infrastructure seeking an exemption from IPPs 1 to 3, 7 and 9, to allow it to collect student enrolment information from the then Department of Education and Children's Services, to assist in the creation of primary school travel plans under the Way2Go Program. The Privacy Committee approved the exemptions for 12 months provided that conditions were applied to limit access to the Geospatial Information Systems (GIS) maps created using student enrolment data.

In December 2009, the Committee approved an extension of the exemptions for a further three years. It also resolved to vary the conditions of the Department of Planning, Transport and Infrastructure's (DPTI) exemption to allow supervised access to the GIS maps. This will allow access to the maps by selected 'focus teachers' in South Australian public schools participating in the Way2Go Program, as well as relevant local government officers for the purpose of supporting the development of school travel plans and improving road safety engineering and infrastructure around schools.

In December 2012, the Privacy Committee approved a further request to extend the exemptions for DPTI and the Department of Education and Child Development for a further three years.

See APPENDIX F for the full text of the exemptions.

3.7.5 South Australian Electoral Roll Dataset

The Privacy Committee dealt with one submission from SA NT DataLink during the year seeking exemptions from IPP 2, 8 and 10. 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 SA NT DataLink's Master Linkage File (MLF).

The Privacy Committee granted exemptions to the Department for Health and Ageing (DHA) and the Electoral Commission of South Australia (ECSA) allowing ECSA disclosure of limited personal information from the South Australian Electoral Roll dataset to DHA officers located within SA NT DataLink, and for DHA to collect and use the personal information. The information was to be used only for the establishment of the MLF, with the information being de-identified by a unique and random code.

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

3.7.6 Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families

The *Information Sharing Guideline for Promoting the Safety and Wellbeing of Children, Young people and their Families* (ISG) was introduced in 2008 to provide a clear framework for sharing information to support early intervention in the protection of children and young people. In May 2008, the Privacy Committee first granted an exemption to agencies required to observe the ISG, by removing the words "and imminent" from IPP 10(b). The exemption was extended for a further two years in May 2009. In April 2011, the Privacy Committee extended the exemption for a further two years.

In June 2013, the Privacy Committee approved a temporary extension of the exemption backdated from 6 April 2013 and expiring 18 September 2013.

See APPENDIX H 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 4 February 2013

Government of South Australia

Cabinet Administrative Instruction No.1 of 1989

(Re-issued 30 July 1992, 18 May 2009 and 4 February 2013)

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 4 February 2013.

(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.

(e) the agency has reason to suspect that unlawful activity has been, is being or may be engaged in, and discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

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 – Post Event Patron Ticketing Information

Exemption – BASS South Australia

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

This exemption applies to BASS South Australia. It is an exemption from compliance with Principle 10, allowing BASS South Australia to disclose event specific patron listings to publically funded arts companies that perform in Adelaide Festival Centre venues.

The publically funded arts companies are

- Adelaide Symphony Orchestra
- State Theatre Company of South Australia
- State Opera South Australia
- Windmill Performing Arts
- Brink Productions
- Adelaide Festival
- Australian Ballet
- WOMAdelaide
- Other ARTS SA funded arts organisations

The personal information to be disclosed is:

- Title
- Name
- Address
- Phone Number(s)
- Email Address
- Ticket transaction history (specific to the publically funded arts company receiving the information)

The purpose of the disclosure is to allow BASS South Australia to disclose event specific patron listings to the publically funded arts companies to allow them to contact their patrons to verify the patron's email and contact preferences relative to that company.

All other Principles continue to apply.

Conditions

The exemption from IPP10 will be a once only exemption to allow BASS South Australia to disclose the information to the publically funded arts companies to allow them to contact their patrons to verify the patron's email and contact preferences relative to that company.

The exemption is conditional on

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

- Only the details for patrons that have opted-in to receive information from the publically funded arts companies or have not been asked about their contact preferences will be disclosed to the publically funded companies.
- The details for patrons that have opted-out of receiving information from the publically funded arts companies must not be disclosed to the publically funded companies.
- The publically funded arts companies must make it clear to patrons that their details were provided to them by BASS South Australia as a result of a previous ticket purchase through BASS South Australia.
- Patrons that do not respond to contact from the publically funded arts companies are deems to have opted-out and must not be contacted again unless or until their contact preferences are changed.

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 the information has been disclosed to the publically funded arts companies.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

25 September 2012

APPENDIX D Exemption Granted – Community Protection Panel Alcohol and Other Drug Service Model

Exemption – OCSAR (AGD)

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

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

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

- Name, date of birth, sex, ethnicity
- Number of offences and most serious offence (based on major charge) prior, during and post participation in the AOD
- Health issues (including drug use, physical and/or mental health) as they relate to case management and/or the AOD Service Model
- Periods of detention
- Family and living situation (including those under the Guardianship of the Minister)
- AOD Assessment
- Information about number of family members involved in the AOD program
- Treatment plans and case notes of the young person and family members in the AOD program
- Reported alcohol and drug usage
- Participant response to the AOD intervention process

The purpose of collection and use is to allow OCSAR to undertake an evaluation of CPP AOD Service Model.

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

[2] *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 from the date of approval of 31 October 2012 to 30 June 2013. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

5 November 2012

APPENDIX E Exemptions Granted – Offender Management Plan Pilot Program

Exemption – SAPOL, DCS, DCSI, DHA, AGD, 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[3] (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 (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), Department for Health and Ageing (DHA), Attorney-General's Department (AGD) and the Department of Further Education, Employment, Science and Technology (DFEEST). It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, DHA, AGD 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. This includes the personal information of family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender. The information is collected and held by each agency through its mandated service provision.

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

All other Principles continue to apply.

Conditions

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

This exemption is conditional on the Pilot Practice Guidelines for the Pilot Program being amended to take into account the broader issue of sharing information about an offender's family members and associates. A copy of which is to be provided to the Privacy Committee for information.

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

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

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 applies from the date of its approval until 30 June 2013 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

20 November 2012

Exemption – SAPOL, DCS, DCSI, DHA, AGD, DFEEST, TAFE SA

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 South Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), Department for Health and Ageing (DHA), Attorney-General's Department (AGD), Department of Further Education, Employment, Science and Technology (DFEEST) and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, DHA, AGD, DFEEST and TAFE SA 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. This includes the personal information of family members and associates, where it has been identified that those individuals

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

contribute significantly to the offending lifestyle of the nominated offender. The information is collected and held by each agency through its mandated service provision.

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

All other Principles continue to apply.

Conditions

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

This exemption is conditional on the Pilot Practice Guidelines for the Pilot Program being amended to take into account the broader issue of sharing information about an offender's family members and associates. A copy of which is to be provided to the Privacy Committee for information.

Security of Personal Information

The security of the personal information should be managed in line with the Government's 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 applies from the date of its approval until 30 June 2013 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

3 April 2013

Exemption – SAPOL, DCS, DCSI, DHA, AGD, DFEEST, TAFE SA

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 Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), Department for Health and Ageing (DHA), Attorney-General's Department (AGD), Department of Further Education, Employment, Science and Technology (DFEEST) and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, DHA, AGD, DFEEST and TAFE SA 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. This includes the personal information of family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender. The information is collected and held by each agency through its mandated service provision.

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

All other Principles continue to apply.

Conditions

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

This exemption is conditional on the Pilot Practice Guidelines for the Pilot Program being amended to take into account the broader issue of sharing information about an offender's family members and associates. A copy of which is to be provided to the Privacy Committee for information within 6 months of the date of this exemption.

Security of Personal Information

The security of the personal information should also be managed in line with the Government's 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.

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

- Personal information is protected during transit; electronic information should be encrypted and password protected and physical files should not be left unattended in an unsecure 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 applies from the date of its approval until 30 June 2015 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

26 June 2013

APPENDIX F Exemptions Granted – Way2Go Program

Exemption – 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[6] (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 IPP 10, allowing DECD to disclose personal enrolment information to the Department for Planning, Transport and Infrastructure (DPTI) to the Way2Go Program.

The information to be disclosed for each enrolled student in a participating Way2Go school will be in the form of a de-identified geocode consisting of:

- school of enrolment
- year level
- spatial location of the student's residential address.

The information disclosed will not include the name of the student, their individual class or any other reference.

The purpose of disclosure is to allow DPTI to use the enrolment information and Geospacial Information Systems (GIS) to create maps of student travel routes. The maps will support the development of travel plans for South Australian public primary schools and the improvement of road safety engineering and infrastructure around primary schools.

All other Principles continue to apply.

Conditions

The exemption is restricted to information related to public primary school enrolments in South Australia.

Destruction or retention of personal information

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

Expiry

This exemption is provided for three years, for the period 5 December 2012 to 5 December 2015. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

10 December 2012

---

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

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

This exemption applies to the Department for Planning, Transport and Infrastructure (DPTI). It is an exemption from compliance with IPPs 1,2,3,7 and 9, allowing DPTI to collect personal enrolment information from the Department for Education and Child Development (DECD) and use that information in the administration of the Way2Go program.

The information to be collected for each enrolled student in a participating ***Way2Go*** school will be in the form of a de-identified geocode consisting of:

- school of enrolment
- year level
- spatial location of the student's residential address.

The information collected will not include the name of the student, their individual class or any other reference.

The purpose of disclosure is to allow DPTI to use Geospatial Information Systems (GIS) to create maps of student travel routes. The maps will support the development of travel plans for South Australian public primary schools and the improvement of road safety engineering and infrastructure around primary schools.

All other Principles continue to apply.

Conditions

This exemption is conditional on the personal information collected by DPTI being accessed only by DPTI's Community Education and Programs staff and staff of DPTI's GIS team. This includes limiting access to any maps created using the personal information that indicate the specific location of student home addresses to those staff.

DPTI's Community Education and Programs staff may provide supervised access to the GIS maps to selected 'focus teachers' from relevant South Australian public primary schools for the purposes of developing school travel plans.

DPTI's Community Education and Programs staff may provide supervised access to the GIS maps to relevant local government officers for the purposes of supporting the development of school travel plans and improving road safety engineering and infrastructure around schools. DPTI should ensure that the local government council concerned has a privacy policy in place that is substantially similar to the IPPs or agrees to access the GIS maps subject to compliance with relevant provisions of the IPPs.

No copies of the GIS maps should be made by anyone other than DPTI's Community Education and Programs staff and staff of the DPTI's GIS team. GIS maps should be appropriately classified under the Security Classification Scheme in the South Australian Recordkeeping Metadata Standard.

The exemption is restricted to information related to South Australian public primary school enrolments in South Australia.

---

[7] *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

Data disclosed to DPTI from DECD is to be destroyed or retained in accordance with an approved disposal authority under the *State Records Act 1997*.

The records collected by DPTI, which are duplicates of the official records owned and held by DECD, are to be destroyed following the creation of the associated GIS maps, in accordance with Normal Administrative Practice as described in Government Disposal Schedule 15, issued under the *State Records Act 1997*.

Expiry

This exemption is provided for three years, for the period 5 December 2012 to 5 December 2015. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

10 December 2012

APPENDIX G Exemption Granted – SA NT DataLink - South Australian Electoral Roll dataset

Exemption – Department for Health and Ageing

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

This exemption applies to the Department for Health and Ageing (DHA). It is an exemption from compliance with Principles 2 and 8, allowing DHA to collect and 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 Electoral Commission of South Australia's South Australian Electoral Roll Dataset and is limited to:

- Elector Number
- Title
- Family Name
- Given Names
- Date of Birth
- Country of Birth (3 character code)
- Sex
- Address Line 1, 2 and 3 (including State and postcode)
- Any of the above information provided for other family members and included in these records.

Excluded from the dataset is information relating to 'silent electors' and those individuals who have sought to be 'provisionally enrolled'.

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*.

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

Expiry

This exemption is granted from 20 February 2013 to 19 February 2016. 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

20 February 2013

Exemption – ECSA

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 Electoral Commission of South Australia (ECSA). It is an exemption from compliance with Principle 10, allowing ECSA to disclose personal information to the Department for Health and Ageing (DHA) employees within the Data Linkage Unit of SA NT DataLink.

The personal information to be disclosed is from ECSA's South Australian Electoral Roll Dataset and is limited to:

- Elector Number
- Title
- Family Name
- Given Names
- Date of Birth
- Country of Birth (3 character code)
- Sex
- Address Line 1, 2 and 3 (including State and postcode)
- Any of the above information provided for other family members and included in these records.

Excluded from the dataset is information relating to 'silent electors' and those individuals who have sought to be 'provisionally enrolled'.

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.

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

ECSA 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 20 February 2013 to 19 February 2016. It will be reviewed by ECSA 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

20 February 2013

APPENDIX H Exemption Granted – Information Sharing Guidelines (ISG) for promoting the safety and wellbeing of children, young people and their families

Exemption – all agencies required to observe the ISG

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

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

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

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

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

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

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

Compliance

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

Further Conditions

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

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

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

- the introduction of staff / volunteer induction on the application of the ISG;
- the adoption of appropriate protocols for gaining consent from clients for disclosing personal information.

Expiry

This is a temporary exemption backdated to 6 April 2013 and expiring 18 September 2013.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

26 June 2013