Government of South Australia

Privacy Committee
Of South Australia

# Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2015

Executive Officer
Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 464
ADELAIDE SA 5001
Phone (08) 8204 8786
privacy@sa.gov.au

September 2015

For information and advice, please contact:

The Presiding Member
Privacy Committee of South Australia
c/- State Records of South Australia
GPO Box 464
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 2015. 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.

Simon Froude
**PRESIDING MEMBER**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

30 September 2015

# Table of Contents


**1 Year in Review ..... 4**

**2 South Australian Public Sector Privacy Framework ..... 5**

2.1 The Information Privacy Principles Instruction ..... 5

2.2 The Privacy Committee of South Australia ..... 6

**3 Activities of the Privacy Committee ..... 11**

3.1 Advice to the Minister ..... 11

3.2 Privacy Developments in other jurisdictions ..... 11

3.3 Recommendations and submissions ..... 17

3.4 To make publicly available, information as to methods of protecting individual privacy ..... 21

3.5 Keep informed as to the extent to which the Information Privacy Principles are implemented ..... 22

3.6 Complaints ..... 22

3.7 Exemptions ..... 23

**Appendices ..... 26**

APPENDIX A Information Privacy Principles ..... 26

APPENDIX B Proclamation of the Privacy Committee of South Australia ..... 32

APPENDIX C Exemptions Granted – Multi-Agency Protection Services Project ..... 35

APPENDIX D Exemptions Granted – Youth Justice Data ..... 39

APPENDIX E Exemptions Granted – Centre for Automotive Safety Research ..... 42

# 1 Year in Review

The challenges facing individuals and government agencies in the protection of personal privacy have changed significantly since the Privacy Committee of South Australia (the Committee) was established by Proclamation in 1989. These challenges highlight the necessity to have adequate and effective privacy oversight. This was evident in some of the developments in privacy reform across Australia in the reporting year 2014-15. The Victorian *Privacy and Data Protection Bill* passed into law in September 2014 merging the existing roles of Privacy Commissioner and the Commissioner for Law Enforcement Data Security to create a single Commissioner for Privacy and Data Protection. The Australian Capital Territory's *Information Privacy Act 2014* commenced operation in September 2014. This Act establishes a clear and consolidated privacy framework for the ACT including introducing the Territory Privacy Principles which are consistent with the Australian Privacy Principles.

These developments reinforce the need for a legislative privacy regime in South Australia. South Australia remains one of only two Australian jurisdictions without specific legislation to protect personal information in its public sector.

The Committee remains concerned that South Australia continues to manage privacy through an administrative scheme and remains strongly committed to its position that the privacy of South Australians should be protected by information privacy legislation. Legislation would ensure the personal information of South Australian citizens held by the South Australian public sector is afforded privacy protections consistent with that in other Australian states and territories, by providing a legislated framework for the appropriate collection, use and sharing of personal information.

During 2014-15 the Privacy Committee continued to provide advice and recommendations to the Minister and government agencies on the protection of privacy and the Information Privacy Principles Instruction (IPPI). It also continued to fulfil its role in receiving privacy complaints, responding to privacy enquiries and granting exemptions from the IPPI that it considered in the public interest. During the reporting year, the Privacy Committee extended or granted six exemptions to State Government agencies across three subject areas and concluded two complaints. The executive support to the Privacy Committee handled 231 enquiries from the public and State Government agencies, which represents a 10 per cent increase on the previous year.

This is a report of the activities of the Privacy Committee for the year ending 30 June 2015. 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*. The IPPI includes a set of ten Information Privacy Principles (IPPs) that regulate the way South Australian public sector agencies collect, use, store and disclose personal information.

### 2.1.1 Information Privacy Principles

#### Principles 1-3 – Collection

Personal information must be collected legally, fairly and where relevant. 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 should not be used for another purpose or disclosed to a third party for another purpose unless:

- the person would reasonably expect it to be used or disclosed for that secondary purpose;
- the person has expressly or impliedly consented;
- it is required to prevent a serious threat to the life, health or safety 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;
- the agency suspects unlawful activity has been, is being or may be engaged in and the use or disclosure is necessary for its investigation of the matter or reporting its concerns to relevant persons or authorities; or
- the agency reasonably believes that the use or disclosure relates to information about an individual that suggest that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person;

and the use or disclosure is appropriate in the circumstances; and is made in accordance with guidelines issued by the Minister.

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

The IPPI can be accessed on the Department for the Premier and Cabinet website at http://dpc.sa.gov.au/premier-and-cabinet-circulars, and in Appendix A of this report.

### 2.1.2 Amendments to the Information Privacy Principles Instruction

There were no amendments to the IPPI in 2014-15.

## 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 is 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, and in Appendix B of this Report.

### 2.2.2 Reporting

During 2014-15, the Privacy Committee was responsible to Hon John Rau MP, Deputy Premier and Attorney-General.

### 2.2.3 Membership

Clause 1(2) of the Proclamation of the Privacy Committee establishes membership of the Committee. It requires that the Committee consists of six members, all of whom are to be appointed by the Minister. Of the six members:

- three are nominated by the Minister (one of whom must not be a public sector employee and one must have expertise in information and records management);
- one is to be nominated by the Attorney-General;
- one is to be nominated by the Minister responsible for the administration of the *Health Care Act 2008*; and
- one is to be nominated by the Commissioner for Public Employment.

At the conclusion of the reporting year, the membership of the Committee was as follows:

**Presiding Member:**

- Mr Simon Froude, Acting Director, State Records of South Australia, Department of the Premier and Cabinet - appointed to 11 January 2017.

**Members, in alphabetical order:**

- Ms Kathy Ahwan, Principal Consultant, Policy and Legislation Unit Department of Health and Ageing – appointed to 11 January 2017.
- Ms Deslie Billich, non-public sector employee – appointed to 30 September 2016.
- Mr Peter Fowler, Director, Security and Risk Assurance, Office for Digital Government, Department of the Premier and Cabinet – appointed to 2 February 2016.
- Ms Trish Simpson, Senior Solicitor, Out-posted, Crown Solicitor's Office, Attorney-General's Department – appointed to 22 February 2017.
- Ms Krystyna Slowinski, Manager, Evaluation and Research, Business Affairs, Department for Communities and Social Inclusion – appointed to 1 June 2016.

**Resignations**

During the reporting year, Mr Terry Ryan and Ms Bernadette Quirke tendered their resignations from the Privacy Committee. Mr Andrew Stanley was replaced with Ms Kathy Ahwan.

Mr Terry Ryan, former Director, State Records, was appointed as the Presiding Member of the Committee in September 2002. Mr Ryan was appointed for his expertise in information and records management. Mr Ryan retired from the public sector in August 2014 and resigned as Presiding Member of the Committee in December 2014.

Ms Bernadette Quirke, Legal Counsel in the Commercial Section of the Crown Solicitor's Office, was appointed on the nomination of the Attorney-General in September 2004. Ms Quirke resigned from the Committee in December 2014.

Mr Andrew Stanley was appointed on the nomination of the Minister for Health in July 2002 for his expertise and knowledge of privacy issues in the health sector. My Stanley's appointment expired in December 2014 and he was replaced by the Minister for Health's new nominee, Ms Kathy Ahwan.

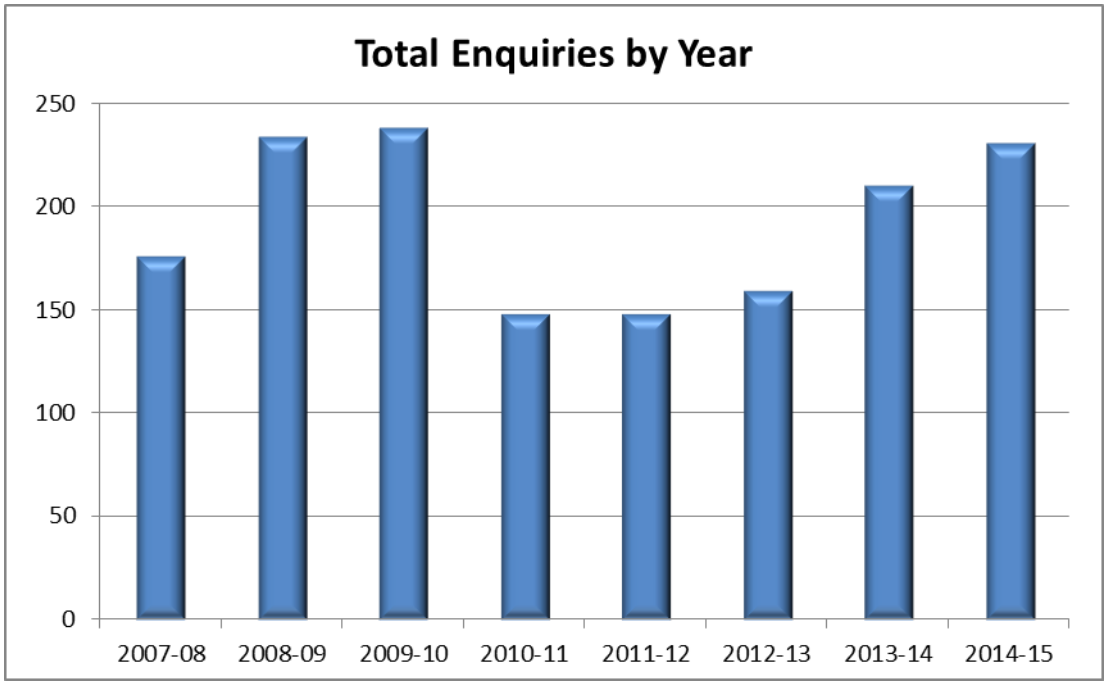
### 2.2.4 Resources

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 one full time equivalent (FTE) staff. Due to resource constraints, the FTE committed to providing executive support was reduced to 0.5 FTE in the second half of 2014-15.

#### 2.2.4.1 Privacy Enquiries

During the reporting year, State Records responded to 231 telephone and email enquiries from the public and State Government agencies relating to all aspects of privacy of personal information. This is 10 per cent higher than the number of enquiries reported in 2013-14.

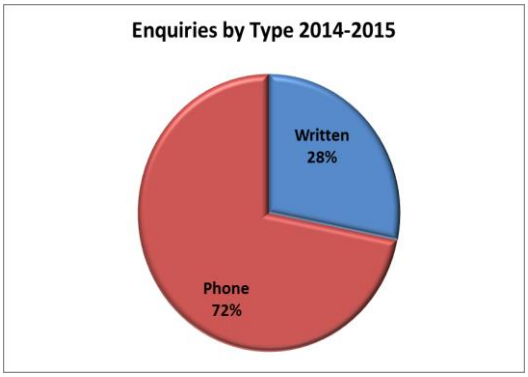
The following chart shows the change in the number of enquiries received over time.

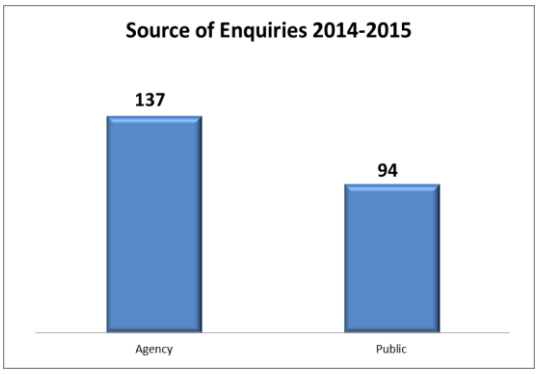



Over the reporting year:

- 70 per cent of all enquiries were dealt with over the telephone.
- The number of enquiries received from the public increased by 11 per cent from 85 in 2013-14 to 94 in 2014-15.
- The number of enquiries received from State Government agencies increased by 10 per cent, from 125 in 2013-14 to 137 in 2014-15.

- Overall, 59 per cent of all enquiries received were from State Government agencies, which is consistent with 2013-14.




#### 2.2.4.2 Privacy Training

State Records offers privacy awareness sessions as well as conducting in-house sessions at the request of State Government agencies. This year resourcing considerations have resulted in State Records being unable to offer regular privacy awareness sessions. However, during the reporting year State Records delivered a privacy presentation at a Local Government Records Management Seminar in February 2015.

### 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 on the Premier and Cabinet website.

Payments for sessional fees for the Privacy Committee during 2014-15 totalled $566.50.

### 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.

A copy of the handbook can be found on the State Records website.

### 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 South Australia can balance its economic, social and environmental aspirations in a way that improves overall wellbeing of the South Australian community, 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 expects 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%, or greater, female membership.

### 2.2.9 Seven Strategic Priorities

In February 2012, the Premier announced the Government's seven strategic priorities. Those 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, the Committee has endorsed the *Information Sharing Guidelines for Promoting Safety and Wellbeing*, and has provided exemptions relating to the Multi-Agency Protection Services Project, SA NT DataLink and the Centre for Automotive Safety Research.

# 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'*.

During the reporting year the Privacy 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 Privacy 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'*.

As the authority responsible for privacy in South Australia, the Privacy Committee receives invitations to respond to government inquiries in addition to other opportunities to comment on draft legislation or plans in other jurisdictions.

In May 2013, the Privacy Committee noted the decision of the South Australian Cabinet to tighten the requirements for submissions to other jurisdictions, including submissions made in response to national inquiries. As such, it is required to seek Cabinet approval for any submission it makes to another jurisdiction.

The Privacy Committee is committed to observing the guidance of the South Australia Cabinet; however, it remains concerned that it will be unable to meet those requirements within most inquiry and consultation timeframes. As a result, the Committee may be unable to contribute to privacy discussions in other jurisdictions.

The Privacy Committee is aware of the following initiatives in other jurisdictions. Further information regarding these initiatives can be sought from the relevant jurisdiction.

### 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. Some of the more significant developments in other jurisdictions are outlined below.

#### 3.2.1.1 Australian Privacy Law Reform

The *Privacy Amendment (Privacy Alerts) Bill 2014* which was introduced into the Federal Parliament on 20 March 2014 is still before the Senate. The Bill aims to amend the Privacy Act to establish a framework for the mandatory notification by

regulated entities of serious data breaches to the Australian Information Commissioner and to affected individuals.

On 2 October 2014, the *Freedom of Information Amendment (New Arrangements) Bill 2014* was introduced into the Federal Parliament. The Bill seeks to amend the *Australian Human Rights Commissioner Act 1986* and the *Privacy Act 1988* to provide for an Australian Privacy Commissioner as an independent statutory office holder within the Australian Human Rights Commission. The Bill also seeks to repeal the *Australian Information Commissioner Act 2010* to abolish the Office of the Australian Information Commissioner (OAIC). The Bill aims to amend 23 Acts including the *Freedom of Information Act 1982*.

In the previous reporting year, the Privacy Committee noted the intention of the Australian Government to disband the OAIC by 1 January 2015. However, as this Bill is still before the Senate, the OAIC will remain operational until further notice.

On 30 June 2015, the OAIC released a Guide to Privacy Regulatory Action, to be read in conjunction with the Privacy Regulatory Action Policy (released November 2014). The guide provides an explanation of the OAIC's privacy regulatory powers and the way in which the OAIC will exercise those powers.[1]

#### 3.2.1.2 New South Wales Reform

Privacy within New South Wales is governed by two principal pieces of legislation, the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002* (HRIP Act). In 2012, amendments were made to the Health Privacy Principles in the HRIP Act. These amendments came into effect in November 2014 and alter the circumstances under which a patient's genetic information can be disclosed to a genetic relative, allowing disclosure in some circumstances without the consent of the patient. For example, this may include where disclosure would *"lessen or prevent a serious threat to life, health, or safety of a genetic relative of the individual to whom the information relates."*[2]

#### 3.2.1.3 Victorian Privacy and Information Security Reforms

In December 2012, the Victorian Government announced a major reform to its privacy regime with its intention to establish a new Privacy and Data Protection Commissioner.

In June 2014, the Committee became aware of the introduction of the *Privacy and Data Protection Bill 2014* (Privacy and Data Protection Bill) into the Parliament of Victoria. The Privacy and Data Protection Bill merges the existing roles of Privacy Commissioner and the Commissioner for Law Enforcement Data Security to create a single Commissioner for Privacy and Data Protection with

---

[1] http://www.oaic.gov.au/news-and-events/news/privacy-news/guide-to-privacy-regulatory-action

[2] http://www.ipc.nsw.gov.au/news-media/news/nsw-genetic-health-guidelines-issued-nsw-privacy-commissioner-result-changes-hrip,

responsibility for the oversight of the privacy and data protection regime in Victoria.

The Privacy and Data Protection Bill passed into law in September 2014.

#### 3.2.1.4 Australian Capital Territory Privacy Law Reform

In March 2014, the Committee became aware that the *Information Privacy Bill 2014* (Information Privacy Bill) had been presented to the Australian Capital Territory's (ACT) Legislative Assembly. The intention of the Information Privacy Bill was to establish a clear and consolidated privacy framework for the ACT including introducing the Territory Privacy Principles which are consistent with the Australian Privacy Principles.

The *Information Privacy Act 2014* was passed by the ACT Parliament in June 2014 and came into effect in September 2014. This legislation regulates the handling of personal information (other than personal health information) by public sector agencies in the ACT. Prior to the introduction of this legislation, the federal Privacy Act applied to ACT Government agencies.

#### 3.2.1.5 National Electronic Health Reform

The Australian Government's commitment to national electronic health reform saw the implementation of the Personally Controlled Electronic Health Record (PCEHR) system in 2012-13.

The PCEHR, now called an eHealth Record system, provides individuals with the opportunity to access their health information when and where they need it and to share this information with relevant healthcare providers. It has the potential to improve efficiency and accuracy of information transfer across the health sector and communication between healthcare professionals, leading to more comprehensive and better quality healthcare services.

Complaints regarding the eHealth Record system are managed in accordance with the *Information Sharing and Complaints Referral Arrangements for the PCEHR between the Office of the Australian Information Commissioner and State and Territory Health and Privacy Regulators* (Arrangements). These Arrangements were finalised and published by the OAIC in June 2013.

The purpose of the Arrangements is to establish an agreed protocol for referral and handling of eHealth Record system complaints. The Privacy Committee previously reported that the South Australian Health and Community Services Complaints Commissioner (HCSCC) is a party to the Arrangements. The Privacy Committee is not a party to the Arrangements as it has no regulatory function; however, it has determined that it will refer any relevant complaints in line with the Arrangements.

During the previous reporting year, the Committee, through the Attorney-General, advised the Minister for Health and Ageing that, should the Committee receive a complaint in relation to the eHealth Record system, it would refer the compliant to the most relevant authority, which may be the HCSCC.

The Committee has not received any complaints in relation to the eHealth Record system since its inception.

In 2013, a review into the PCEHR was conducted, which looked into concerns about the progress of the implementation of the system. A report from this

review was released in May 2014. It sets out 38 recommendations including a proposal to:

- Rename the PCEHR to My Health Record (MyHR).
- Restructure the approach to governance by dissolving the National E-Health Transition Authority (NEHTA) and replace it with the Australian Commission for Electronic Health (ACeH).
- Transition to an 'opt-out' model for all Australians on their MyHR to be effective from a target date of 1st January 2015.
- Commission an Information Security Risk Assessment of the end-to-end flow of consumer information to and from the MyHR platform.
- Add a flag to the clinical author to identify if their patient has restricted or deleted a document in their MyHR to facilitate a discussion on the clinical impact.[3]

Public consultation was undertaken with respect to these recommendations between July and September 2014. The consultation process identified concerns associated with an opt-out system; primarily around the question of implied consent and potential privacy risks.

In May 2015, a Privacy Impact Assessment Report (PIA) was released, with specific attention to the privacy implications of an opt-out model. The PIA identified a number of privacy issues relating to an opt-out model including the need for individuals to be informed about how their information will be handled, and how they can opt-out and adjust privacy control settings with respect to their health information. The PIA made a number of recommendations including:

- amendments to the Personally Controlled Electronic Records Act 2012 and the Health Care Identifiers Act 2010; and
- improving ways to reach and inform vulnerable and disadvantaged individuals.[4]

Trials of an opt-out model are set to begin in July 2016, with work currently underway to select trial sites.

#### 3.2.1.6 Australian Law Reform Commission Inquiries

**Serious Invasions of Privacy in the digital era**

On 12 June 2013, the Commonwealth Attorney-General asked the Australian Law Reform Commission (ALRC) to conduct an inquiry into the protection of privacy in the digital era. The inquiry's Terms of Reference required that it address both prevention and remedies for serious invasions of privacy.

On 3 September 2014, the ALRC's final report, *Serious Invasions of Privacy in the Digital Era*, was tabled in Parliament.

---

[3] http://health.gov.au/internet/main/publishing.nsf/Content/17BF043A41D470A9CA257E13000C9322/$File/FINAL-Review-of-PCEHR-December-2013.pdf (p15-17)

[4] http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/21C511E1CC1A6850CA257E7600208E8D/$File/PCEHR%20Opt%20Out%20PIA%20-%202015.pdf (page 6)

"The ALRC was asked to design a statutory cause of action for serious invasions of privacy, and also to consider other innovative ways in which law may reduce serious invasions of privacy in the digital era."[5]

The report explores arguments for effectively filling the gaps in privacy legislation by amending and expanding current legislation versus formulating new privacy specific legislation. The ALRC determined that the latter was a more appropriate course of action, and one of the sixteen recommendations is to establish a new tort in new Commonwealth legislation. Other key recommendations include:

- the establishment of new commonwealth surveillance legislation to replace existing state and territory laws; and
- extending the powers of the Privacy Commissioner to enable the Commissioner to investigate complaints and refer matters to court for enforcement.[6]

#### 3.2.1.7 Invitations from other jurisdictions

During the reporting year the Presiding Member of the Privacy Committee was invited to attend a National Privacy Commissioners' Forum to be held at the Commonwealth's Attorney-General's Department (Commonwealth AGD) in Canberra on 8 July 2015.

The purpose of the forum was to bring together Privacy Commissioners (or equivalent) from each jurisdiction to discuss and ascertain the potential privacy impacts associated with the design and functions of the central Interoperability Hub of the forthcoming National Facial Biometric Matching Capability (Capability).

The forum discussions and separate consultations were to assist in informing a privacy impact assessment (PIA) of the Capability. Commonwealth AGD is establishing the Capability to allow participating agencies to share and match facial images such as those used on identity documents like passports, visas and driver licences. The Capability would be used by agencies to achieve fraud detection, law enforcement, national security, service delivery and community safety outcomes. The central Hub will allow participating Commonwealth, state and territory agencies with the lawful authority to transmit facial recognition match requests and responses between themselves.

The Presiding Member was unable to attend but the Commonwealth AGD offered to keep South Australia informed about developments in this area.

### 3.2.2 International Privacy Developments

#### 3.2.2.1 Privacy Rights under International Law

In 2012, The European Commission (the Commission) launched a program to reform data protection rules in the European Union (EU). The current data protection rules date back to 1995, and there is a great need to bring those rules in line with modern technologies and practices.

---

[5] http://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123

[6] http://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123/recommendations

In June 2015 it was announced that the Justice Council supported the Commission's proposal on new data protection rules. It was announced that negotiations between the Commission, European Parliament and the Council were to begin in June 2015, with a strong commitment to deliver the new data protection rules to the EU by the end of 2015.

In June 2015, the Commission also released findings from the Eurobarometer Data Protection Survey. Some statistics gathered are as follows:

- Two-thirds of the respondents (67%) say that they are worried about having no control over the information they provide online, while only 15% feel they have complete control.
- Six out of ten respondents say that they do not trust online businesses (63%), or phone companies and internet service providers (62%).[7]

### 3.2.3 Meetings and seminars

#### 3.2.3.1 Asia Pacific Privacy Authorities

Asia Pacific Privacy Authorities (APPA) 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.

The Committee has observer status at APPA. However, due to budget constraints, the Committee has not been represented at APPA in the last three financial years.

The most recent meeting (43rd) of APPA was held on 11–12 June 2015 and hosted by the Office of the Privacy Commissioner for Personal Data, Hong Kong.

APPA members provided jurisdictional reports on matters such as legal reform, law enforcement, mandatory data breach notification, privacy training and child and youth privacy programs. Other agenda items included global privacy developments, privacy implications of big data, online behavioural advertising and investigations, and accountability as the basis for privacy compliance in technology innovations.

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

#### 3.2.3.2 Privacy Authorities of Australia

Privacy Authorities of Australia (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.

A teleconference between PAA communications officers was held in August 2014 but the Privacy Committee was not represented due to resource constraints.

[7] http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm

## 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 Australian Early Development Census – 2015 Collection

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 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 five key areas of childhood development; physical health and wellbeing, social competence, emotional maturity, language and cognitive skills (school based), and communication skills and general knowledge.

In early 2012, the South Australian Department for Education and Child Development (DECD) sought an exemption from the IPPI to enable it to disclose identified personal information of South Australian reception aged children to the Commonwealth for the purposes of pre-population of the AEDI Survey.

As reported in the Privacy Committee's Annual Report for 2012-13, the Committee did not support the submission. It was the Committee's view that de-identified data was all that was required to fulfil the primary purpose of the AEDI Survey. Despite the Committee's concerns, the personal information was disclosed to the Commonwealth. The Committee considered this a breach of the IPPI. As noted in the Report, the Committee is committed to continuing to work through its concerns with DECD and the Commonwealth prior to the next collection in early 2015.

In November 2014, DECD wrote to the Privacy Committee to request an exemption from the IPPI to disclose personal information for the purposes of the Australian Early Development Census (AEDC). As part of its participation in the AEDC collection for 2015, DECD proposed to disclose personal information from its enrolment data to the Social Research Centre (SRC), a contracted service provider of the Australian Department of Education.

The Committee considered the request for exemption at its meeting in December 2014 and determined that although the disclosure of enrolment information to the SRC as proposed would not comply with IPPI 10, it could comply if disclosure was conducted on the basis of informed consent.

In order for DECD to justify that parents have provided informed consent to the disclosure of their children's information, the Committee made a number of recommendations including that AEDC checklist questions are clearly accessible from the AEDC parent's website, parents are provided with more information about the questions and how to opt-out, and DECD and its school principals take

reasonable steps to ensure parents receive a letter informing them of the collection.

DECD responded to the Committee in January 2015 stating that it would work with the Australian Government Department of Education to implement the recommendations made by the Committee.

### 3.3.2 SA Water Concession Scheme

In July 2014, SA water sought an exemption from the IPPI to enable SA Water to provide access to its customer database to the Department for Communities and Social Inclusion (DCSI) for the purposes of administering the South Australian Concession Program. DCSI also sought an exemption to collect and use the information.

DCSI administers concessions on behalf of the Government for household water and sewerage rates, council rates and/or an energy concession. SA Water traditionally administered this concession function on behalf of DCSI. The Committee previously provided an exemption for this to occur in December 2008.

SA Water advised that allowing DCSI access to its Customer Service Information System (CSIS) enables DCSI to manage the concession program in a more efficient manner. SA Water's application for exemption requested that DCSI be given access to all of SA Water's customer details through CSIS, not just concession customers. Further information provided by SA Water suggested that it could not audit or monitor access to the CSIS by DCSI staff as they were provided with read only access.

In November 2014, the Committee wrote to SA Water to advise it recognised the public interest in the efficient processing of Government concessions however, on balance, the exemption could not be granted unless SA Water could demonstrate it could manage DCSI access to personal information in a secure way.

SA Water wrote to the Committee in December 2014 stating that it had further investigated options to address the Committee's concerns and that it was willing to develop a secure search facility to limit DCSI access to account property information for concession customers. Access to other accounts would be processed manually.

The Committee agreed that this approach would comply with the IPPI and therefore no exemption was required.

### 3.3.3 Police Drug Diversion Initiative

In April 2010, the Privacy Committee granted South Australia Police (SAPOL) and the Drug and Alcohol Services SA (DASSA) an exemption from the IPPI for the collection and disclosure of personal information under the Police Drug Diversion Initiative (PDDI). The exemption was granted for four years, expiring in April 2014.

In November 2014, SAPOL and DASSA wrote to the Privacy Committee to request an extension of the exemption for a further five years.

The PDDI refers adults and young people who have been detected by a police officer for simple possession drug offences to a health based intervention with an

accredited health professional, rather than processing them through the justice system.

The Committee considered the request for a further exemption and was of the view that subject to improvement of the information provided by SAPOL to offenders upon collection of their personal information, it appeared that the PDDI process complied with the IPPI and did not require a further exemption. The Committee wrote to both SAPOL and DASSA to advise an exemption was not required, provided that SAPOL include a statement on or with the Drug Diversion referral form that states:

- the collection of personal information on the form (in respect of adults) is a collection required by the *Controlled Substances Act 1984*; and
- the personal information collected will be disclosed between SAPOL, DASSA and their contracted service providers for the purpose of facilitating and monitoring health based interventions provided under the PDDI.

The Committee further recommended that SAPOL and/or DASSA take reasonable steps to ensure the guardians of any persons under the age of 18 who are referred under the PDDI are provided with a copy of the Referral Notice.

On 2 January 2015, the Commissioner of Police wrote to the Committee indicating that SAPOL would implement the Committee's recommendations in early 2015.

### 3.3.4 SA NT DataLink – Data Integration Unit

SA NT DataLink is an unincorporated joint venture comprising the South Australian and Northern Territory Governments and a number of non-government organisations and SA universities. 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 for each research project enabled by SA NT DataLink.

In February 2015, SA-NT Datalink approached the Privacy Committee to seek in-principle support for establishing the Data Integration Unit (DIU) which would store de-identified data from data custodians and provide access to the required data to researchers for approved research projects. The establishment of the DIU would assist with the increasing demand for de-identified data, issues regarding security of the data, and issues relating to the timeliness of access experienced by researchers.

The current process for providing researchers with linked data involves SA NT DataLink receiving personal information from agencies, analysing and linking common records by random alpha numeric keys and storing this data in SA NT DataLink's MLF. By establishing the DIU the identifying information held and managed in the MLF will be separated from the service use and clinical information in the DIU. The DIU will be physically and electronically separate.

The Privacy Committee acknowledged the need to address resource pressures on data custodians and the expectations of researchers who require access to datasets quickly. The Committee was satisfied with the security arrangement of the DIU and agreed to support the proposal. SA NT DataLink agreed to keep the Committee informed of the DIU implementation and consult with the Committee on the development of relevant principles and processes.

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

### 3.3.5 SA Pathology – Surveillance Cameras

In December 2014, *The Advertiser* reported that SA Pathology used covert surveillance cameras to record the activities of workers in its mailroom. It was reported that SA Pathology had since replaced the covert cameras with visible surveillance cameras. It was further reported that the Minister for Health had asked the Chief Executive of SA Health to conduct an investigation into the use of the cameras.

In March 2015, *ABC News* published an online article regarding the results of SA Health's investigation into the use of the surveillance cameras. It was reported that the investigation found no laws had been breached; however the decision to install covert cameras was a "lapse in judgement by SA Pathology management".

The Privacy Committee considered the matter at its February and March 2015 meetings and decided to write to SA Health seeking further explanation and clarification. In its response, SA Health explained that a covert camera was installed in the print room of SA Pathology's Consumer Products Unit due to concerns regarding the tampering of pathology reports and/or printing equipment and a second covert camera was installed in the reception area for safety and security reasons.

The covert cameras had no audio capability and once the matter was brought to his attention, the Chief Executive of SA Health instructed SA Pathology to remove the cameras. The footage from the cameras has since been destroyed.

A policy regarding the use of video surveillance in SA Health is currently under development. SA Health has agreed to formally consult the Privacy Committee on its draft policy as soon as practicable.

### 3.3.6 DECD – Scanning Fingerprints

In February 2015, *Adelaide Now* reported that East Para Primary School advised parents, by way of an electronic newsletter, that their children would have their

fingerprints scanned as part of a new student attendance record-keeping program.

It was reported that the system would allow students to register attendance and allow the school to manage roll books more efficiently. The article stated that the school advised parents that concerns about privacy were unwarranted as the program did not store fingerprints but instead created a template of the unique fingerprint characteristics. Fingerprints cannot be recreated by the template. The template is digitized and encrypted.

The Committee considered the practice of scanning fingerprints. The Committee agreed that fingerprinting was a collection of personal information but that it was not an unlawful or unfair collection. Parents also have the option to exclude their children from the program.

The Committee wrote to both DECD and the East Para Primary School to inquire about whether there is a policy in place regarding scanning fingerprints and to ensure that parents and staff are provided with all relevant information, including how fingerprints templates are stored securely.

The Committee is continuing to work with DECD on developing a policy.

### 3.3.7 SA Police – Use of Remotely Piloted Aircraft Systems

In March 2015, SAPOL approached the Privacy Committee to discuss SAPOL's use of Remotely Piloted Aircraft Systems (RPAS). SAPOL had developed a draft policy stipulating how RPAS are to be used and in what circumstances.

At the Committee meeting in July 2015, the Committee considered the RPAS policy and provided feedback to SAPOL.

## 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. The Privacy Committee will continue to look at ways it can improve its performance of this function in 2015-16 within its limited resources.

### 3.4.1 Guidelines and Information Sheets

The following agency guidelines and information sheets were updated with links to the new State Records website:

- Privacy Guidelines for SA Government Websites and Online Applications
- Privacy and Cloud Computing Guideline
- Privacy and Open Data Guideline
- Amendment to the Information Privacy Principles Instruction
- Contracting and the Information Privacy Principles

- Information Privacy Principles and Child Protection Information Sheet
- Short guide to the Information Privacy Principles

#### 3.4.2 Participation in committees and groups

When the opportunity arises, the Privacy Committee is represented at meetings with Commonwealth, State and Territory Governments as deemed appropriate to promote the protection of individual privacy. This includes representation on, or involvement with, the:

- South Australian Government's ICT Security and Risk Steering Committee
- Security Managers Round Table
- Cyber Taskforce
- National Identity Security Coordination 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 IPPI and, in some cases, this is a condition of an exemption. In addition, under the terms of the IPPI, 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 IPPI.

### 3.5.1 Privacy Breaches

#### 3.5.1.1 Northern Adelaide Local Health Network

On 2 March 2015, *ABC News* reported that the Lyell McEwin Hospital had inadvertently released medical notes to a member of the public relating to three other patients. The Lyell McEwin Hospital is part of the Northern Adelaide Local Health Network (NALHN).

State Records commenced an investigation into this matter in March 2015 and has agreed to provide a copy of its findings to the Privacy Committee once complete.

In April 2015, the Privacy Committee wrote to the Chief Executive of NALHN to advise it would review the findings of the State Records' investigation before considering the matter in full from a privacy perspective. As of 30 June 2015, the investigation was still ongoing.

## 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 Committee may also refer matters to the Independent Commission Against Corruption, via the Office for Public Integrity, should it consider a matter to fall within its jurisdiction of misconduct or maladministration.

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 sectors to resolve privacy complaints and improve practices when handling personal information.

There were five formal complaints received during the reporting year, two of which had been concluded at the end of the year. A summary of the concluded complaints is outlined in the table below.

### 3.6.1 Complaints Concluded Summary Table

| | Respondent Organisation | Information Privacy Principle (IPP) | Outcome |
|---|---|---|---|
| 1 | Government Department | IPP 10 – Disclosure of personal information to third party | Concluded |
| 2 | Government Department | IPP 4 – Storage of personal information | Concluded |

## 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 IPPI, 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 granted exemptions across three subject areas throughout the reporting year. Following is a summary of each request for exemption.

### 3.7.1 Multi-Agency Protection Services Project

In July and October 2014 and again in June 2015, the Privacy Committee considered requests from SAPOL seeking an exemption from compliance with the IPPI to allow for the collection, use and disclosure of personal information for the purposes of the Multi-Agency Protection Services (MAPS) Pilot Project.

The purpose of the MAPS Project is to share information and intelligence between a number of agencies to protect victims, or potential victims, of domestic violence and/or child protection referrals.

The Committee granted extensions in July and October 2014 to the exemption granted in June 2014 to allow SAPOL to undertake a review and evaluation of the MAPS Project in early 2015. In June 2015, SAPOL requested that the Committee again extend its exemption for a further 12 months to allow the Project to continue concurrent with the finalisation of a Cabinet submission seeking approval for the project's future progression and funding. The Committee agreed, out of session, to grant an interim extension of six months upon the condition that representatives from the MAPS Project attend a Committee meeting to address some concerns raised by the Committee, including the longevity of the pilot project and the security of transferring information between participating agencies.

See Appendix C for the full text of the exemptions.

### 3.7.2 Youth Justice Data

In January 2015, SA NT DataLink and the Department for Communities and Social Inclusion (DCSI) sought a three year exemption from the IPPI.

The SA NT DataLink System aims to provide an improved evidence base to enable statistical linkage projects to be undertaken to improve the health and wellbeing of South Australians and Northern Territorians and the general population.

Youth Justice Data is routinely collected by DCSI as part of its service delivery function in relation to working with children and young people. The addition of the DCSI Youth Justice data to SA NT DataLink Master Linkage File (MLF) will enable timely and relevant research that will lead to improved understandings of the associations and outcomes in relation to issues confronting children and young people. It may also lead to improved policies, programs and services that help children and young people access opportunities to participate safely and productively in the community and desist from offending.

The Privacy Committee approved an exemption to allow DCSI to disclose personal information to SA NT DataLink and an exemption to allow SA NT DataLink to use the information to expand the MLF. The Committee was satisfied that use and disclosure of this type of information is similar to other information already provided to SA NT DataLink.

See Appendix D for the full text of the exemptions.

### 3.7.3 Centre for Automotive Safety Research

In February 2015, SAPOL sought an exemption from the IPPI so it could provide the Centre for Automotive Safety Research (CASR) with personal information of people involved in vehicle collisions to assist CASR to conduct in-depth research and interviews.

CASR conducts in-depth crash investigation research that assists in the identification and evaluation of alternative corrective road safety measures. CASR proposes to develop and explore further the current trends related to crash involvement in order to develop more targeted road safety countermeasures.

The Privacy Committee approved an exemption for SAPOL to allow disclosure to CASR of the names and telephone numbers of individuals involved in crashes to enable CASR to obtain consent for the collection of further personal information.

Recently in July 2015, the Committee considered a request from SAPOL to broaden this exemption to include other personal information, in particular the address of individuals involved in collisions. The Committee agreed to grant a broader exemption on the conditions that letters sent to individuals asking for their consent explain how CASR came to be in possession of their address and other personal information, and that CASR maintains research ethics approvals from SA Health and the University of Adelaide.

See Appendix E for the full text of the exemptions.

# 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 16 September 2013**

**Government of South Australia**

**Cabinet Administrative Instruction No.1 of 1989**

**(Re-issued 30 July 1992, 18 May 2009, 4 February 2013, 5 August 2013 and 16 September 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 16 September 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 Act 2009.*

(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.

“Minister” means the Minister who is, for the time being, responsible for the Instruction.

"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 (the secondary purpose) unless:

(a) the record-subject would reasonably expect the agency to use the information for the secondary purpose and the secondary purpose is related to the primary purpose of collection;

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

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

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

(e) 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;

(f) 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; or

(g) the agency reasonably believes that the use relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and

(i) the agency reasonably believes that the use is appropriate in the circumstances; and

(ii) the use complies with any guidelines issued by the Minister for the purposes of this clause.

(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 for a purpose that is not the purpose of collection (the secondary purpose) unless:

(a) the record-subject would reasonably expect the agency to disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose of collection;

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

(c) 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 of some other person;

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

(e) 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;

(f) 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; or

(g) the agency reasonably believes that the disclosure relates to information about an individual that suggests that the individual has engaged or may engage in illegal conduct or serious misconduct in relation to a person; and

(i) the agency reasonably believes that the disclosure is appropriate in the circumstances; and

(ii) the disclosure complies with any guidelines issued by the Minister for the purposes of this clause.

**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**

Independent Commissioner Against Corruption

Motor Accident Commission (formerly State Government Insurance Commission)

Office for Public Integrity

South Australian Asset Management Corporation

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 Exemptions Granted – Multi-Agency Protection Services Project

### Exemption – SAPOL, DCS, SA Health, DCSI, 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 (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), SA Health, Department for Communities and Social Inclusion (DCSI) including the Office for Women, and Department for Education and Child Development (DECD) including Families SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, SA Health, DCSI and DECD to share information and intelligence as part of SAPOL's Multi-Agency Protection Services (MAPS) Project. This exemption replaces the exemption issued on 17 June 2014. (Document reference D14/03800)

The personal information to be shared will include given and family name, address (including previous addresses), gender, age, date of birth, ethnicity and any other relevant personal information held by MAPS partner agencies. This includes personal information of victims and potential victims, offenders, associates and dependents. The personal information is collected and held by each agency through normal and accepted business processes.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the MAPS Project in the protection of victims, or potential victims, of domestic violence and/or child protection matters through earlier identification of children and victims at risk.

All other Principles continue to apply.

### Conditions

This exemption is conditional on SAPOL and partner agencies seeking Cabinet approval for the ongoing operation of the MAPS Project, including the collection, use and disclosure of relevant personal information, prior to the expiration of this exemption.

### 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 Information Security Management Framework, and the agency's security management systems and practices. 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 unsecure environment.

- Personal information collected under the MAPS Project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the MAPS Project, or when delivering services to an individual 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 28 July 2014 until 30 January 2015, or the end of the MAPS Project, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
**A/Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

14 August 2014

**Exemption – SAPOL, DCS, SA Health, DCSI, 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 (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), SA Health, Department for Communities and Social Inclusion (DCSI) including the Office for Women, and Department for Education and Child Development (DECD) including Families SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, SA Health, DCSI and DECD to share information and intelligence as part of SAPOL's Multi-Agency Protection Services (MAPS) Project. This exemption replaces the previous exemption provided to these agencies in relation to the MAPS Project on 14 August 2014 (D14/04784).

The personal information to be shared will include given and family name, address (including previous addresses), gender, age, date of birth, ethnicity and any other relevant personal information held by MAPS partner agencies. This includes personal information of victims and potential victims, offenders, associates and dependants. The personal information is collected and held by each agency through normal and accepted business processes.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the MAPS Project in the protection of victims, or potential victims, of domestic violence and/or child protection matters through earlier identification of children and victims at risk.

All other Principles continue to apply.

### 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 Information Security Management Framework, and the agency's security management systems and practices. 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 unsecure environment.
- Personal information collected under the MAPS Project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the MAPS Project, or when delivering services to an individual 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 29 October 2014 until 30 June 2015, or the end of the MAPS Project, whichever is earlier.

Simon Froude
**A/Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

4 November 2014

### Exemption – SAPOL, DCS, SA Health, DCSI, 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 (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), SA Health, Department for Communities and Social Inclusion (DCSI) including the Office for Women, and Department for Education and Child Development (DECD) including Families SA. It is an exemption from compliance with IPPs 2, 7, 8 and 10, allowing SAPOL, DCS, SA Health, DCSI and DECD to share information and intelligence as part of SAPOL's Multi-Agency

Protection Services (MAPS) Project. This exemption follows on from the previous exemption granted in October 2014 and expiring on 30 June 2015 (D14/06019).

The personal information to be shared will include given and family name, address (including previous addresses), gender, age, date of birth, ethnicity and any other relevant personal information held by MAPS partner agencies. This includes personal information of victims and potential victims, offenders, associates and dependants. The personal information is collected and held by each agency through normal and accepted business processes.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the MAPS Project in the protection of victims, or potential victims, of domestic violence and/or child protection matters through earlier identification of children and victims at risk.

All other Principles continue to apply.

**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 Information Security Management Framework, and the agency's security management systems and practices. 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 unsecure environment.
- Personal information collected under the MAPS Project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the MAPS Project, or when delivering services to an individual 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 1 July 2015 until 31 December 2015, or the end of the MAPS Project, whichever is earlier.

Simon Froude
**Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

29 June 2015

## APPENDIX D Exemptions Granted – Youth Justice Data

### Exemption – SA NT DataLink

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

This exemption applies to SA NT DataLink. It is an exemption from compliance with Principle 8, allowing SA NT DataLink to use personal information from the Department for Communities and Social Inclusion (DCSI) for a purpose that was not the purpose of the collection of that information.

The personal information to be used is from DCSI, Youth Justice, and is limited to:

- Unique record identifier (i.e. episode reference number)
- Unique person identifier where available
- Given name(s) (including all 'akas', aliases and nicknames)
- Date of birth
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Country of birth
- Full address including geocodes where available
- The full name and date of birth of the mother and father of the child or young person where available.

The information is to be used for the creation of master linkage keys as part of the SA NT Data Linkage System by the Data Linkage Unit.

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 SA Health within the Data Linkage Unit.

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

### Security

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 Information Security Management Framework, and the agency's security management systems and practices.

**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 18 February 2015 to 18 February 2018. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
**Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

27 February 2015

**Exemption – DCSI**

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

This exemption applies to the Department for Communities and Social Inclusion (DCSI), Youth Justice. It is an exemption from compliance with Principle 10, allowing DCSI, Youth Justice to disclose personal information to SA NT DataLink.

The personal information to be disclosed by DCSI, Youth Justice, is limited to:

- Unique record identifier (i.e. episode reference number)
- Unique person identifier where available
- Given name(s) (including all 'akas', aliases and nicknames)
- Date of birth
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Country of birth
- Full address including geocodes where available
- The full name and date of birth of the mother and father of the child or young person where available.

The information is to be disclosed for the creation of master linkage keys as part of the SA NT Data Linkage System by the Data Linkage Unit.

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 SA Health within the Data Linkage Unit.

DCSI, Youth Justice remains responsible for the secure transfer and storage of personal information in line with the IPPs.

**Security**

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 Information Security Management Framework, and the agency's security management systems and practices.

**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 18 February 2015 to 18 February 2018. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
**Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

27 February 2015

## APPENDIX E Exemptions Granted – Centre for Automotive Safety Research

### Exemption – SAPOL

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles (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). It is an exemption from compliance with Principle 10 allowing SAPOL to disclose personal information to the Centre for Automotive Safety Research (CASR).

The personal information to be disclosed by SAPOL to CASR is limited to:

- Family and given names of persons involved in vehicle collisions
- Telephone number(s) of persons involved in vehicle collisions

The information to be disclosed is for the purpose of allowing CASR to make contact with persons involved in a vehicle collision to enable CASR to gain consent to interview and obtain further information from such persons.

All other Principles continue to apply.

### Conditions

The information disclosed is only to be used by CASR for the purpose of contacting persons involved in a vehicle collision to gain their consent to interview such persons and obtain further information relevant to the research being undertaken by CASR.

SAPOL is responsible for the secure transfer of personal information in line with the IPPs.

### Security

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 Information Security Management Framework, and the agency's security management systems and practices.

### 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 18 February 2015 to 18 February 2016. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
**Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**
27 February 2015

**Revised Exemption – SAPOL (granted in the reporting year 2015-16)**

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

This revised exemption applies to the South Australia Police (SAPOL). It is an exemption from compliance with Principle 10 allowing SAPOL to disclose personal information to the Centre for Automotive Safety Research (CASR).

The personal information to be disclosed by SAPOL to CASR relates to the personal information of persons involved in vehicle collisions, and includes those persons:

- Family and given names
- Address
- Gender
- Date of birth
- Age
- Licence number
- Licence state
- Licence status
- Phone numbers
- Seatbelt status
- Helmet status
- Hospital
- Injury level
- Breath analysis result
- BAC level
- Vehicle registration number
- Vehicle year and make

The information to be disclosed is for the purpose of allowing CASR to obtain important information about collisions and to make contact with persons involved in collisions to enable CASR to gain consent to conduct in-depth interviews. Interviews greatly assist CASR to gain a better insight into vehicle accidents and to form a clearer picture of what occurred.

All other Principles continue to apply.

**Conditions**

This revised exemption is granted on the following conditions:

- information disclosed to CASR is only to be used by CASR for the purpose of obtaining further information relevant to the research being undertaken and for contacting persons involved in vehicle collisions to gain their consent to be interviewed;

- the letter sent to persons involved in vehicle collisions for the purpose of gaining their consent explains how CASR came to be in possession of their address and other personal information; and
- CASR maintains current research ethics approvals from the University of Adelaide and SA Health.

SAPOL is responsible for the secure transfer of personal information in line with the IPPs.

**Security**

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 Information Security Management Framework, and the agency's security management systems and practices.

**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 revised exemption replaces the previous exemption issued on 27 February 2015 and applies from 8 July 2015 to 18 February 2016. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
**Presiding Member**
**PRIVACY COMMITTEE OF SOUTH AUSTRALIA**

27 July 2015