Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2014

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

September 2014

For information and advice, please contact:

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

ph: (08) 8204 8786
fax: (08) 8204 8777
email: privacy@sa.gov.au

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

The Hon John Rau MP
ATTORNEY-GENERAL

Dear Attorney-General

The Privacy Committee of South Australia is pleased to provide you with this report of its activities for the year ending 30 June 2014. 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
A/PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

30 September 2014

Table of Contents

1 Year in Review

2013-14 represented another challenging year for the Privacy Committee of South Australia (Committee). The year saw significant developments in privacy reform across Australia, including reforms to the Commonwealth's *Privacy Act 1988* which came into effect on 12 March 2014. The Act establishes a new set of Australian Privacy Principles (APPs) to guide the handling of personal information in Commonwealth Government agencies and some private sector organisations. It also increases the accessibility of personal information for credit reporting purposes and provides greater enforcement powers for the Commonwealth Privacy Commissioner. These changes will have an impact on all South Australians.

Victoria and the Australian Capital Territory (ACT) also progressed their privacy reforms. In June 2014 the *Privacy and Data Protection Bill 2014* was introduced into the Parliament of Victoria, and the ACT Parliament passed the *Information Privacy Bill 2014*.

These developments highlight and reinforce the need for a legislative privacy regime in South Australia.

The Committee is pleased that some significant changes were made to the State's administrative scheme for information privacy, the Information Privacy Principles Instruction (IPPI), as a result of the Independent Education Inquiry. But it remains concerned about the ability of the IPPI to provide an adequate framework for protecting personal information in South Australian government agencies. The concerns arise from:

- the increased focus of government to deliver services collaboratively and online;
- the further technological development in government information systems such as the Department for Health and Ageing's Electronic Patient Administration System and the Australian Government's eHealth Record System;
- the increased use of surveillance technologies; and
- the ongoing threat of cyber-crime in Australia.

It should be noted that the IPPI was developed at a time when coordinated service provision in government was not the norm, information was primarily held in paper files and the internet in Australia was still in its infancy.

During the reporting year the South Australian Law Reform Institute released an Issues Paper *Too Much Information: a statutory cause of action for invasion of privacy* and the Australian Law Reform Commission commenced an inquiry into the protection of privacy in the digital era. In addition, the 68th General Assembly of the United Nations approved a draft resolution on 'the right to privacy in the digital age'. This demonstrates a strong interest in protecting the right to privacy, and particularly digital privacy, not only nationally but internationally. Also of note are the results of the Office of the Australian Privacy Commissioner's *Community Attitudes to Privacy Survey – Research Report 2013*, which identified that there is an increasing awareness of privacy legislation in the community.

These significant privacy reforms and inquiries serve to reinforce the need to reform South Australia's administrative scheme for privacy. South Australia remains one of only two Australian jurisdictions without specific legislation to protect personal information in its public sector.

The Committee is 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. It remains the Committee's view that the development and implementation of information privacy legislation in South Australia could be expected to improve awareness of protections in place for personal information provided to the South Australian Government. Legislation would also ensure the personal information of South Australian citizens that is 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.

The Privacy Committee continued to provide advice and recommendations to the Minister and government agencies on the protection of privacy and the IPPI. It also continued to fulfil its role in receiving privacy complaints, responding to privacy enquiries and granting exemptions from the information privacy principles that it considered in the public interest. During the reporting year, the Privacy Committee extended or granted 14 exemptions from the IPPs to State Government agencies across 5 subject areas (see item 3.7), concluded four complaints (see item 3.6) and contributed to a number of consultation programs and inquiries (see items 3.2 and 3.3). The executive support to the Privacy Committee handled 210 enquiries from the public and State Government agencies, which is 32 per cent higher than the number of enquiries handled in the previous year (see item 2.2.4).

This is a report of the activities of the Privacy Committee for the year ending 30 June 2014. 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 IPPs are not intended to prevent disclosure of personal information where it is in the public interest to do so, such as a serious threat to the life, 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

In August 2013, the Government amended the IPPI in response to the Independent Education Inquiry (see also 3.3.7) and to improve information handling and sharing by government agencies. The IPPI was further amended in September 2013 to alter the agencies to which the IPPI does not apply.

2.1.2.1 Disclosure for the Primary Purpose of Collection

Clause 4(10) of the IPPs was amended to allow for the disclosure of personal information for the primary purpose of collection. If information is collected for a particular purpose, it can also be disclosed for that purpose.

2.1.2.2 Reasonably Expected Secondary Use or Disclosure

Clauses 4(8) and (10) were amended to include a new subclause (a) to permit the use and disclosure of personal information for the primary purpose of collection and for a secondary purpose that is related to the primary purpose of collection, if the record-subject would reasonably expect the agency to use or disclose the information for that secondary purpose.

2.1.2.3 Serious Threats to Life, Health or Safety

Clauses 4(8) and (10) were amended to remove the necessity for a serious threat to be imminent. They were also amended to make clear that they include threats to the safety of a person as well as life or health.

2.1.2.4 Illegal Conduct or Serious Misconduct in Relation to a Person

Clauses 4(8) and (10) were amended to include a new subclause (g) to permit the use and disclosure of information about an individual that might reveal that the individual has engaged in, or may engage in, illegal conduct or serious misconduct in relation to a person. Information can only be used or disclosed where an agency reasonably believes that the use or disclosure is appropriate in the circumstances and it complies with guidelines to be issued by the Minister. To date there have been no Ministerial Guidelines developed under this clause.

2.1.2.5 Exempt Agencies

The IPPI was amended to include the Independent Commissioner Against Corruption (ICAC) and the Office for Public Integrity (OPI) as agencies to which the IPPI does not apply.

2.2 The Privacy Committee of South Australia

2.2.1 Establishment and Functions

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

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

A copy of the Proclamation can be found following the IPPI, and in Appendix B of this Report.

2.2.2 Reporting

During 2013-14, 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*
- 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 Terry Ryan, Director, State Records of South Australia, Department of the Premier and Cabinet - appointed to 5 December 2014[1].

Members, in alphabetical order:

- Ms Deslie Billich, non-public sector employee – appointed to 30 September 2014.
- Mr Peter Fowler, Director, Security and Risk Assurance, Office of the Chief Information Officer, Department of the Premier and Cabinet – appointed to 2 February 2016.
- Ms Bernadette Quirke, Legal Counsel, Crown Solicitor's Office, Attorney-General's Department – appointed to 5 December 2014.
- Ms Krystyna Slowinski, Manager, Evaluation and Research, Business Affairs, Department for Communities and Social Inclusion – appointed to 1 June 2016.
- Mr Andrew Stanley, nominee of the Minister for Health, non-public sector employee – appointed to 5 December 2014.

Resignations

During the reporting year, Mr Andrew Mills and Ms Nancy Rogers tendered their resignations from the Privacy Committee.

Mr Mills was appointed to the Privacy Committee in November 2008. As the then Chief Information Officer, Mr Mills was appointed for his experience in information technology. Mr Peter Fowler was appointed to fill the vacancy created by Mr Mills' resignation. Mr Fowler is employed by the Office of Chief Information Officer and has considerable experience in information security. Mr Fowler was Mr Mills' nominated proxy.

Ms Rogers was appointed to the Privacy Committee in April 2006. Ms Rogers was appointed for her expertise in privacy issues in the areas of social policy and research ethics. Ms Krystyna Slowinski was appointed to fill the vacancy created by Ms Rogers' resignation. Ms Slowinski is employed by the Department of Communities and Social Inclusion and has considerable experience in social policy and research ethics. Ms Slowinski was Ms Rogers' nominated proxy.

2.2.4 Resources

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

---

[1] *Mr Ryan commenced extended leave in March 2014. Mr Ryan's proxy, Mr Simon Froude, A/Director, State Records was endorsed by Privacy Committee members on 1 April 2014 to act as the Presiding Member of the Privacy Committee of South Australia in Mr Ryan's absence.*

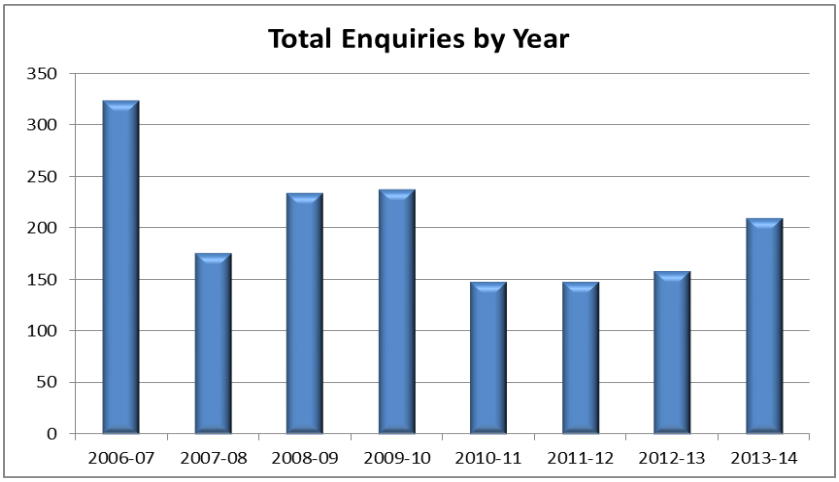
2.2.4.1 Privacy Enquiries

During the reporting year, State Records responded to 210 telephone and email enquiries from the public and State Government agencies relating to all aspects of privacy of personal information. This is 32 per cent higher than the number of enquiries reported in 2012-13.

In March 2014 amendments to the Commonwealth *Privacy Act 1988* came into effect. There was an increase in the number of telephone and written enquires from the public and State Government agencies regarding the effect of these amendments.

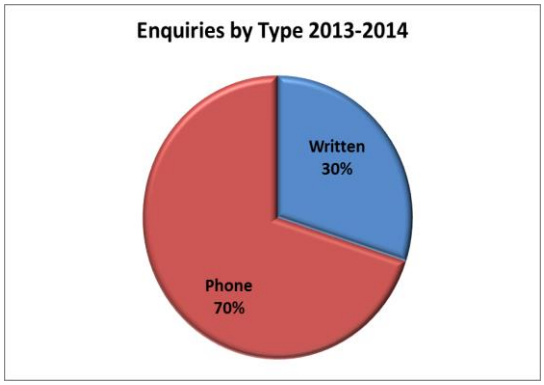
These enquiries were, however, limited to March and April 2014 so, whilst they have contributed, they are not the only reason for the overall increase in enquiries received.

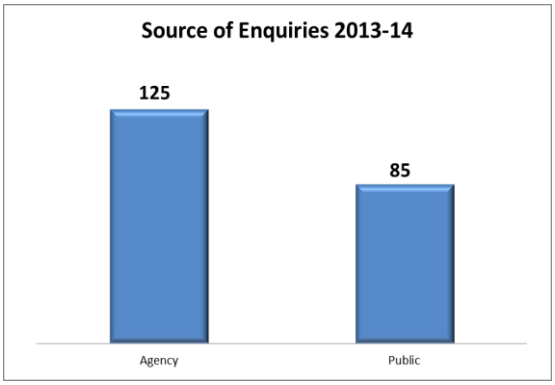
The following chart shows the change in the number of enquiries received over time.



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 37 per cent from 62 to 85 reported in 2013-14.
- the number of enquiries received from State Government agencies increased by 33 per cent, from 94 in 2012-13 to 125 in 2013-14.
- Overall, 60 per cent of all enquiries received were from State Government agencies, which is consistent with 2012-13.





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 privacy awareness sessions. As State Records did not receive any requests for agency specific sessions there were no privacy awareness sessions conducted in the 2013-2014 reporting year.

As reported last year, privacy awareness has previously been included in the curriculum for the nationally accredited Certificate III in Recordkeeping developed and delivered by State Records, in partnership with TAFE SA. Certificate III in Recordkeeping is no longer offered by State Records and it is unknown if privacy awareness components are incorporated in the Certificate III in Recordkeeping courses offered by other registered training organisations.

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 2013-14 totalled $103.

2.2.6 Meetings

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

2.2.7 Guidelines for members

A handbook for members contains information on the role of the Privacy Committee, its relationship to other approval and advisory bodies, duties and obligations of members, the process for handling complaints, and other information of value to members in performing their role. It also includes a brief history of privacy law and self-regulation in South Australia, and an overview of the protection of personal information in other Australian jurisdictions. The handbook was updated in March 2014.

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% female membership.

2.2.9 Seven Strategic Priorities

In February 2012, the Premier announced the Governments 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 Offender Management Plan Pilot Program, Multi-Agency Protection Services Project, Innovative Community Action Network, and SA NT DataLink.

3 Activities of the Privacy Committee

3.1 Advice to the Minister

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

Throughout the reporting year, the Privacy Committee briefed the Minister on a range of matters relating to privacy. This included briefings concerning privacy reform in South Australia, amendments to the IPPI, the Australian Early

Development Index, Biometric Scanning in South Australian Prisons, and the Personally Controlled Electronic Health Record System.

During the year the Committee continued to support the Minister and Government in the development of information privacy legislation for the South Australian public sector. The Committee specifically provided advice to support the project to develop the legislation. The Committee remains concerned about the absence of a legislative framework for information privacy in the South Australian public sector.

3.2 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 numerous 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, meaning it will be unable to contribute to privacy discussions in other jurisdictions.

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

The Privacy Committee is committed to keeping itself informed of the outcome of these initiatives during 2014-15.

3.2.1 Commonwealth, States and Territories

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

3.2.1.1 Australian Privacy Law Reform

On 29 November 2012, the Australian Parliament passed the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which was the Australian Government's response to the Australian Law Reform Commission's (ALRC) *Report 108* on Australian privacy law and practice.

These amendments to the Commonwealth *Privacy Act 1988* (Privacy Act) came into force on 12 March 2014.

The Privacy Act was amended to achieve three key reforms. The first was the establishment of the Australian Privacy Principles (APPs) that replace the two existing sets of privacy principles. The APPs guide the handling of personal information in both Commonwealth Government agencies and private sector organisations. The second was the revision of the credit reporting provisions to make it easier for individuals to access and correct their credit information and allow banks and financial institutions to see an increased amount of information about individual credit histories. The third was to increase the powers of the Commonwealth Privacy Commissioner to enforce the Privacy Act.

As discussed previously, the Privacy Committee noticed a marked increase in the number of enquiries received from State Government agencies and members of the public as a result of the commencement of the Commonwealth's Privacy Act. While it is not uncommon for the Committee to receive requests of this type throughout the year, the increase in enquiries seemed to indicate that some public sector employees are either not aware of the information privacy regime in place within South Australia, or believe that the Commonwealth Act applies to them. As a result, the Committee recommended that a government-wide email be circulated reminding agencies of the requirement to comply with the IPPI.

During the reporting year the Committee became aware of the introduction of the *Privacy Amendment (Privacy Alerts) Bill 2014* into the Federal Parliament. The Bill is a private members bill, introduced by Senator Singh in the Senate on 20 March 2014. It 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.

The Committee also became aware during the reporting year that the Office of the Australian Information Commissioner (OAIC) will be disbanded by 1 January 2015. It is understood that the Privacy Act will continue to be administered by the Privacy Commissioner.

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

The Privacy and Data Protection Bill also addresses a number of the data security issues identified by the Victorian Auditor-General in his 2009 *Report on Maintaining the Integrity and Confidentiality of Personal Information*, including measures to ensure that government handles personal information securely and consistently.

3.2.1.3 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 newly introduced APPs, adapted to ACT circumstances.

The Information Privacy Bill was passed by the ACT Parliament in June 2014. The *Information Privacy Act 2014* (ACT Act) is intended to commence on 11 December 2014.

The main purpose of the ACT Act is to introduce specific ACT privacy legislation to regulate the handling of personal information (other than personal health information) by public sector agencies in the ACT. Presently the federal Privacy Act applies to ACT Government agencies and is administered by the OAIC on behalf of the ACT Government.

3.2.1.4 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 communication of clinical information between healthcare professionals to provide more comprehensive and quality healthcare services. This includes the potential for more efficient and accurate transfer of health information across the health sector.

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 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.

3.2.1.5 Community Attitudes to Privacy Survey

In July 2013 the OAIC commissioned a survey to 'measure Australians' changing awareness and opinions about privacy, as well as their expectations in relation to the handling of their personal information[2].

In October 2013 the OAIC released the survey results in its report *Community Attitudes to Privacy Survey – Research Report 2013*. The survey found that:

- 48% of participants believed that online services posed the biggest privacy risk, 23% felt that identity fraud and identity theft posed the biggest risk followed by data security at 16%.
- an increasing proportion of Australians have been affected, or know someone who has been affected, by identity fraud and identity theft, with 69% of participants being concerned that they will be a victim in the next year.
- 97% of participants believe that using personal information for a purpose other than for which the information was given is inappropriate.
- 80% of participants believe that sending their personal information offshore is a misuse of that information, and 90% are concerned about the practice.
- Australian's have more trust in government than they do in private enterprise, with 60% of Australians deciding not to deal with a private company as a result of their concerns about how their personal information will be used.
- 23% of participants will not deal with a public organisation as a result of their concerns about how their personal information will be used.
- 96% of participants believed that individuals should be advised if their personal information is lost and how personal information is handled and protected.
- The proportion of individuals prepared to have their information shared is rising, with 66% of participants prepared to accept their doctor discussing their health information with other health professionals.

The Privacy Committee believes that the findings of the survey are an important indicator of the community's attitude towards privacy, and notes that the report found an increasing awareness of privacy legislation and possibly other consumer protection laws.

3.2.1.7 South Australian Law Reform Institute

In December 2013, the Privacy Committee received an invitation from the South Australian Law Reform Institute (SALRI) to a call for submissions on whether there should be a statutory cause of action for invasions of personal privacy.

The Issues Paper, *Too Much Information: a statutory cause of action for invasion of Privacy* (Issues Paper) considered whether the remedies available under the current laws were effective in an era of rapid technological change, and asks whether a new cause of action is needed to protect personal privacy.

---

[2] *Community Attitudes to Privacy Survey Research Report,* p 3.

The Committee determined it was unable to develop a submission before the final date for submissions and advised SALRI accordingly. The Committee did, however, provide a link to a copy of its response to the Commonwealth's issues paper published in September 2011, *A Commonwealth Statutory Cause of Action for Serious Invasions of Privacy*.

The Privacy Committee looks forward to considering the outcome of the SALRI review.

3.2.1.8 Australian Law Reform Commission Inquiries

Serious Invasions of Privacy in the digital era

On 12 June 2013, the Commonwealth Attorney-General Mark Dreyfus QC asked the ALRC to conduct an inquiry into the protection of privacy in the digital era. The inquiry's Terms of Reference required that it address both prevention and remedies for serious invasions of privacy. The first stage of public consultation regarding the inquiry occurred in October 2013, with the release of the *Serious Invasions of Privacy in the digital era – Issues paper 43*. A subsequent discussion paper, *Serious Invasions of Privacy in the Digital Era – Discussion Paper 80* was released in March 2014.

The ALRC approached the Committee in February 2014 seeking to meet with representatives in relation to the inquiry. Representatives of the Committee met with staff from the ALRC via teleconference in April 2014 to discuss the five elements of action raised in the discussion paper.

The ALRC was due to deliver its final report to the Attorney-General in June 2014. At the close of the reporting year, the final report was yet to be published.

3.2.1.9 Other invitations for submissions to other jurisdictions

During the reporting year the Privacy Committee received a number of invitations to respond or comment on various initiatives, reviews and proposed amendments to legislation. These included, but were not limited to, the National Cooperative Intelligent Transport System policy paper, the terms of reference for the review of the *Telecommunications (Interception and Access) Act 1979*, the *Student Identifiers Bill* and the *Crimes Act 1914*.

The Committee determined in these cases not to respond, but is committed to noting any outcomes of these reviews.

3.2.2 International Privacy Developments

3.2.2.1 Privacy Rights under International Law

On 26 November 2013, the 68th General Assembly of the United Nations approved a draft resolution on 'the right to privacy in the digital age'. This is a significant development in clarifying privacy rights internationally. This resolution establishes that human rights should prevail irrespective of the medium and, therefore, need to be protected.

The approval of the resolution would have the General Assembly call upon Member States to review their procedures, practices and legislation on the surveillance of communications, their interception and collection of personal data, including mass surveillance, with a view to upholding the right to privacy by ensuring the full and effective implementation of all relevant obligations under international human rights law[3]. Australia is a signatory to the International Covenant on Civil and Political Rights (ICCPR). As a signatory to the ICCPR, Australia recognises that under Article 17, no-one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence, nor to unlawful attacks on his honour or reputation.

Resolution 68/167 *The right to privacy in the digital age* was adopted by the General Assembly on 18 December 2013. The full text of the Resolution can be found at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

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 two financial years.

The last meeting of APPA, the 40th APPA forum, occurred on 26-27 November 2013 in Sydney and hosted by the Office of the Australian Information Commissioner.

Agenda items of particular interest to the Privacy Committee included global privacy developments, unmanned aircraft systems (drones), data in public registers and big data.

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.

The PAA group did not meet in 2013-2014.

[3] United Nations Media Release of the 68th General Assembly, Third Committee, 51st & 52nd Meetings.

3.3 Recommendations and submissions

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

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

3.3.1 Adelaide Fare Collection System (MetroCard and Seniors Card)

In mid-2012, the Seniors Card Unit in the then Department for Health and Ageing (DHA) distributed new Seniors Cards with embedded metrocard technology for use on the Adelaide public transport ticketing system.

In June 2012, the Privacy Committee granted an exemption to allow DHA to disclose personal information of Seniors Card holders to the Department of Planning Transport and Infrastructure (DPTI) for the purpose of ensuring card holders could access all levels of DPTI customer service.

Following an enquiry from a member of the public in January 2013, the Committee became concerned that Seniors Card holders had not been provided with adequate information about the implications of the new Seniors Card and about their options to travel anonymously on public transport. Of particular concern, it appeared that the information regarding the new card on websites maintained by DHA and the Office for the Ageing (OFTA) was inconsistent.

The Privacy Committee engaged with both agencies in relation to its concerns, who committed to addressing the adequacy of publically available information.

In September 2013, the Privacy Committee further reviewed the agencies websites. This review found that the websites now provided enough information to allow Seniors Card holders to understand the implications of using their Seniors Card on public transport, as well as other inconsistencies rectified.

3.3.2 SA NT DataLink

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.

The Privacy Committee continued to work with SA NT DataLink in 2013-14 to ensure appropriate governance in the maintenance and development of the MLF. Of particular interest in 2013-14, the Privacy Committee granted an exemption from the IPPs to permit the addition of identifying variables from the SA Cervix Screening Program dataset to the MLF. In providing this exemption the Privacy Committee deemed that there was significant public interest in doing so given the potential research that would be enabled through data linkage using the dataset.

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

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

3.3.3 Identity Security and Information Privacy

Identity security management is essential for the Government to achieve streamlined integrated and accessible services to citizens and business. Identity security management has strong links with information privacy protection when considering the potential for identity theft or fraud.

In 2013-14 the Privacy Committee continued to provide advice to the Government to support the implementation of the National Identity Security Strategy (NISS). The purpose of the NISS is to guide a national approach to ensure Australians are able to confidently enjoy the benefits of a secure and protected identity.

The Privacy Committee is also represented on the National Identity Security Coordination Group (NISCG). The NISCG is a consultative and representative group for states and territories in the roll out of the NISS, and includes initiatives such as the Document Verification Service (DVS). During the reporting year, the Privacy Committee noted the expansion of access to the DVS to private sector organisations.

3.3.4 Australian Early Development Index

The Australian Early Development Index (AEDI) is a national progress measure for the National Early Childhood Development Strategy, an initiative of the Council of Australian Governments. AEDI is also a key target (T12) of South Australia's Strategic Plan.

AEDI involves the collection of information to help create a snapshot of children's development in communities across Australia every three years. The collection requires teachers to complete a survey for each child in their first year of full-time school. The survey measures the 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 IPPs 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 2013 the Committee was contacted by The Sunday Mail, following the publication of the Committee's 2012-13 Annual Report. The Sunday Mail sought, and was provided with, information regarding the type of information that had been disclosed by DECD.

In May 2014 the Committee met with representatives from DECD and the Commonwealth Department of Education to discuss consent and the Privacy Impact Assessment of the 2012 AEDI collection.

DECD has agreed to continue to work with the Committee in the lead-up to the next AEDI collection in 2015.

3.3.5 Biometric Scanning in South Australian Prisons

In July 2013 the Privacy Committee was made aware by the Office of the Attorney-General of concerns raised by the Law Society of South Australia (Law Society) about the privacy impacts of the use of biometric technology in South Australian prisons.

The Law Society was concerned that the use of biometric technology is a significant intrusion on its members who must visit prisons as part of their role representing clients and as Officers of the Court. The Law Society also noted that the Department for Correctional Services (DCS) is subject to the IPPI, but that the IPPI does not have the force of law and there were no penalties if it is breached. The Law Society, therefore, recommended that a legislative framework for privacy is required to protect the personal information collected. The Law Society recommended, in the interim, that DCS develop and implement a privacy policy regarding biometric technology in prisons.

The Privacy Committee wrote to DCS a number of times on this matter in the reporting year. Specifically the Committee asked DCS to address the requirements of Principle 2 (Collection) of the IPPs. In addition, the Committee sought further details about compliance with the Information Security Management Framework and information provided to visitors to prisons about the biometrics system. The Committee also drew DCS's attention to its record keeping obligations under the *State Records Act 1997*.

In its responses, DCS advised the Committee of its intention to amend the *Correctional Services Act 1982* to include specific references to the use, storage and sharing of information obtained via the Biometric Enrolment System, as well as provisions for sanctions for misuse. DCS also advised that it would review all information provided to visitors and commence scoping and drafting a privacy policy. DCS agreed to consult the Committee on its draft policy. At the close of

the reporting year DCS had not sought the Committee's comment on its draft privacy policy relating to biometric technology and the agency's website had not been updated.

3.3.6 Housing SA – single housing register

The Department for Communities and Social Inclusion (DCSI) sought advice from the Privacy Committee in December 2013 as to whether the IPPI permits the exchange of limited customer information for the purpose of meeting customer's housing needs as part of the implementation phase of its Access Project. The Access Project is designed to make it easier for customers to access social housing services and products through Housing SA, the community housing sector, and Specialist Homelessness Services.

DCSI was advised of the provisions of subclause (a) of Principles 8 and 10 of the IPPI in relation to whether the record-subject would reasonably expect the agency to use or disclose the information for the secondary purpose, and if that secondary purpose is related to the primary purpose.

It was agreed that the exchange of limited customer information as part of the Access Project would not be in breach of the IPPI.

3.3.7 Independent Education Inquiry

Former Supreme Court Justice Honourable Bruce Debelle's Independent Education Inquiry (Inquiry) Report was presented to the Government on 21 June 2013.

As part of its response to the issues considered by the Inquiry, the Government amended the IPPI on 5 August 2013. A summary of the amendments can be found in section 2.1.2.

The amendments were made to permit further information sharing by specific public sector agencies to promote the protection of children, young people and vulnerable adults.

As a result of the amendments to the IPPI, the Privacy Committee issued an information sheet *Amendments to the Information Privacy Principles Instruction* and updated the information sheet *Short Guide to the Information Privacy Principles*.

In April 2014 the Privacy Committee also released a Guideline *Information Privacy Principles and Child Protection*, which outlines the way in which the IPPI works within the State's child protection framework.

3.3.8 Information Sharing Guidelines for Promoting Safety and Wellbeing

Originally called the *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families* (ISG), the ISG was established in 2008 to promote appropriate and timely sharing of information to lessen or prevent risks to the safety and wellbeing of children, young people and their families.

The ISG promotes early intervention and service coordination to prevent harm, and encourages information sharing with the consent of the person to whom the information relates where it is safe and reasonable in the circumstances. Where

it is not safe or reasonable to obtain consent, the ISG provides a framework for appropriate information sharing without consent.

During the 2013-14 reporting year, the Privacy Committee noted the online publication of an updated *Information Sharing Guidelines for Promoting Safety and Wellbeing*. The Committee was later made aware of concerns raised by SA Health regarding the updated ISG and application of it by non-government organisations. The Privacy Committee will continue to monitor progress of updates to the ISG.

3.3.9 Privacy Guidelines for SA Government Websites and Online Applications

In 2001 the Privacy Committee published guidelines to assist agencies to develop privacy statements for government websites.

During the reporting year the Privacy Committee published its *Privacy Guidelines for South Australian Government Websites and Online Applications* Guideline. This Guideline replaces the original guidance published in 2001.

3.3.10 Privacy and Cloud Computing Guideline

In the last reporting year the Office of the Chief Information Officer (OCIO) advised the Privacy Committee of its intention to adapt the Commonwealth's *Cloud Computing Better Practice Guides* for use within the South Australian Government. The Privacy Committee agreed to develop guidance on privacy as it relates to cloud computing in South Australian Government agencies.

The Committee subsequently published the *Privacy and Cloud Computing Guideline* in October 2013.

3.3.11 Privacy and Open Data Guideline

During the reporting year the Privacy Committee was asked by the OCIO to develop guidance on privacy as it relates to open data, as part of the Government's Open Data Action Plan.

The Committee subsequently published the *Privacy and Open Data Guideline* in February 2014, which is part of a collection of resources coordinated by the OCIO.

3.3.12 Information Security Guidance for South Australia public sector agencies

During the reporting year, the Privacy Committee was made aware of, and provided advice in response to, information security related matters. This included:

- Data Breach Guidelines – Managing the notification of those affected when data is compromised
- PSMF Guideline 1 Data Breaches – notifying those affected
- Data Breaches – Numbers you need to know contact sheet
- Information Security brochures

3.3.13 Surveillance Devices Bill 2012

The *Surveillance Devices Bill 2012* (Surveillance Devices Bill) was introduced into the South Australian Parliament on 5 September 2012. The Surveillance Devices Bill seeks to establish a new law to regulate the use of surveillance devices in South Australia to replace the existing *Listening and Surveillance Devices Act 1972* (LSDA).

The Surveillance Devices Bill was referred to the Legislative Review Committee (LRC) in February 2013, to consider:

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

In April 2013 the Privacy Committee was invited to make a submission to the LRC Inquiry. The Committee made a submission on 29 April 2013, which broadly supported the Government's introduction of the Surveillance Devices Bill. It noted that the Surveillance Devices Bill addresses a gap in the provisions of the current LSDA by regulating a broader range of listening and surveillance devices, including provisions for tracking and data surveillance devices.

Following consideration of the Committee's submission, the Privacy Committee was invited to appear before the LRC to provide further evidence. The Committee instead responded in writing to the LRC's specific questions in August 2013.

The final *Report of the Legislative Review Committee into Issues Relating to Surveillance Devices* was tabled in Parliament on 13 November 2013.

The Privacy Committee noted the introduction of the Bill into the Legislative Council on 5 June 2014. The Committee will keep itself informed of the progress of the Bill in 2014-15.

3.3.14 Transport Regulation User Management Processing System (TRUMPS)

On 4 December 2013, *The Advertiser* reported that DPTI had disciplined two staff in relation to misuse of the Transport Regulation User Management Processing System (TRUMPS). The Privacy Committee consequently wrote to DPTI seeking information as to the steps that have been, or were intended to be, taken as a result of the alleged misuse of the TRUMPS systems as reported in *The Advertiser*.

In January 2014, the Privacy Committee received a complaint from a member of the public advising that DPTI had previously refused to remove their electronic signature from the TRUMPS database. The Complainant was concerned that it

could be used fraudulently. The complaint was also referred to DPTI for response.

DPTI's responses to the Committee on this matter included explanation of the range of anti-fraud and anti-corruption controls in place to mitigate the possibility of fraudulent behaviour, and discussion of the need to retain signatures for identification purposes.

Advice was also received from State Records which indicated that the removal of an electronic signature from the TRUMPS database would be an offence under Section 17 of the *State Records Act 1997.*

In dealing with this matter, the Committee recommended to DPTI that it explain, via its website and in other visitor information, that electronic signatures are stored in the TRUMPS database for the life of the individual. DPTI has advised the Committee that it will consider this recommendation.

The Committee advised the complainant that the requirements of the *State Records Act 1997* meant that their electronic signature could not be removed from the database. Further, retention of electronic signatures is required for the reduction of the potential for identity fraud.

The complainant was advised that the Committee was satisfied that DPTI had taken appropriate steps to reduce the likelihood of a driver's electronic signature being used fraudulently.

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 2014-15 within its limited resources.

3.4.1 Participation in committees and groups

When the opportunity arises, the Privacy Committee is represented at meetings with Commonwealth, State and Territory Governments as deemed appropriate to promote the protection of individual privacy. This includes representation on, 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 IPPs and, in some cases, this is a condition of an exemption. See section 3.3 for further information. In addition, under the terms of the IPPs, the Committee may on its own initiative appoint a person to investigate or assist in the investigation of the nature and extent of compliance with the IPPs.

3.5.1 Privacy Breaches

3.5.1.1 Women's and Children's Health Network

In November 2013, the Privacy Committee received a complaint regarding the disclosure of personal information to a contracted service provider for the purpose of debt collection.

The complainant had contacted the contracted service provider and, whilst the issues relating to the recovery of the debt were later resolved, the complainant remained dissatisfied with the service provider's advice regarding the incorrect linkages to personal information in the account history for the purposes of debt collection.

The Privacy Committee referred the complaint to the Women's and Children's Health Network (WCHN). The WCHN advised that, as a result of the complaint, it had taken steps to ensure that the disclosure of personal information in this manner does not reoccur. The steps taken include compliance with recognised debt collection guidelines, review of internal approval processes for debt collection, staff training and additional controls for clarifying information.

The Privacy Committee was satisfied that the WCHN had taken appropriate steps to ensure that the disclosure of personal information in this manner does not occur in the future.

The complainant was consulted and agreed for one part of their complaint to be referred to the Health and Community Services Complaints Commissioner (HCSCC) for investigation. The Committee will keep itself informed as to the outcome of the HCSCC investigation.

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

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

3.6.1 Complaints Concluded Summary Table

	Respondent Organisation	Information Privacy Principle (IPP)	Outcome
1	Government Department	IPP 10 – Disclosure of personal information to third party	Referral to OPI – Concluded
2	Government Department	IPP 10 – Disclosure of personal information to third party	Concluded
3	Government Health Unit	IPP 10 – Disclosure of personal information to third party	Concluded
4	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 IPPs, or where otherwise warranted by unique circumstances. Exemptions are generally subject to conditions, such as an expiry date, an approval from an appropriate

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

The Privacy Committee granted 14 exemptions across 5 subject areas throughout the reporting year. Following is a summary of each request for exemption.

3.7.1 Innovative Community Action Networks Flexible Learning Options Program

In August 2013, the Privacy Committee granted exemptions from the IPPs to enable the evaluation of the impact of the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) Program on the offending behaviour of participants. Specifically, the exemptions were from IPP 10 to allow DECD, SAPOL and CAA to disclose personal information of ICAN FLO participants to the Office of Crime Statistics and Research (OCSAR); and from IPPs 2 and 8 to allow OCSAR to collect and use personal information of ICAN FLO participants from DECD, SAPOL and CAA.

The Committee was later requested to amend the exemptions between OCSAR and DECD to include gender in the list of variables. The amendment to the exemptions was approved out-of-session in September 2013.

See APPENDIX C for the full text of the exemptions.

3.7.2 Memorandum of Understanding for statistical monitoring, information dissemination and statistical analysis

In 2007, the Privacy Committee granted exemptions from IPPs 2, 8 and 10 to enable SAPOL to disclose and OCSAR to collect and use unit record data for the purposes of statistical monitoring, research and evaluation projects, in line with a Memorandum of Understanding (MoU) between the agencies. Those exemptions expired in June 2012.

In August 2013, the Privacy Committee approved exemptions from IPPs 2, 8 and 10 for an additional 5 year period.

See APPENDIX D for the full text of the exemptions. A synopsis of the MoU is available upon request.

3.7.3 SA Cervix Screening Program

The Privacy Committee dealt with one submission from SA NT DataLink, in December 2013, seeking an exemption from IPPs 2, 8 and 10. The exemption was sought in line with the governance arrangements established between the Privacy Committee and SA NT DataLink to facilitate the development and operation of SA NT DataLink's Master Linkage File (MLF).

The Privacy Committee granted the exemption to SA Health, enabling the SA Cervix Screening Program within SA Health to disclose identified data to SA Health officers within the Data Linkage Unit of SA NT DataLink, and for the information to be collected and used for a purpose that was not the purpose of collection.

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

3.7.4 Offender Management Plan Pilot Program

An initial exemption was granted by the Privacy Committee in March 2010 to allow for information sharing between selected agencies in relation to the Offender Management Plan (OMP) Pilot Program.

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

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

Further exemptions were granted in April and June 2013 which extended the length of the exemption and amended the agencies to which the exemption applies.

In April and May 2014 the Committee considered a further request from SAPOL to include DECD as a participating agency in the OMP Pilot Program. The Committee determined to grant a limited exemption to DECD and the other participating agencies to share information of the children of one particular offender. The Committee also required that, prior to the disclosure of the children's personal information, the consent of one or both of the children's legal guardians is sought. Only in circumstances where consent is not granted, or if it is given and then later revoked, does the exemption apply.

At that time, the Committee also varied the existing exemption to include a condition that consent is sought from family members and associates for their personal information to be shared as part of the OMP Pilot Program. Only in circumstances where consent is not granted, or if it is given and then later revoked, does the exemption apply.

See APPENDIX F for the full text of the exemptions.

3.7.5 Multi-Agency Protection Services Project

In May and June 2014 the Committee considered a request from SAPOL seeking an exemption from compliance with IPPs 2, 8 and 10 to allow for the collection, use and disclosure of personal information for the purposes of the Multi-Agency Protection Services (MAPS) Project.

The purpose of the MAPS Project is to share information and intelligence for the purpose of protecting victims, or potential victims, of domestic violence and, or child protection referrals.

The Committee granted a six month exemption from compliance with the IPPs, allowing SAPOL, DCS, SA Health, DCSI and DECD to collect, use and disclose personal information for the purposes of the MAPS Project.

The exemption is conditional upon SAPOL and the MAPS partner agencies seeking Cabinet approval for the proposal.

See APPENDIX G and for the full text of the exemption.

Appendices

APPENDIX A Information Privacy Principles

Cabinet Administrative Instruction 1/89, also known as the Information Privacy Principles (IPPs) Instruction, and premier and cabinet circular 12, AS AMENDED BY CABINET 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 – Innovative Community Action Networks Flexible Learning Options Program

Exemption – DECD

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

This exemption applies for the study period 2006 to 2010 for the Department for Education and Child Development (DECD). It is an exemption from compliance with Principle 10, allowing DECD to disclose personal information of participants in the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and were not enrolled in 2010. The information is to be disclosed by DECD to the Office of Crime Statistics and Research (OCSAR) for the purposes of evaluating the ICAN FLO program.

The personal information to be disclosed is:

- Name
- Date of Birth
- FLO enrolment dates
- Geographical area of school enrolment
- Whether the student is Aboriginal
- Whether the student had a disability
- Whether the student was under the Guardianship of the Minister

The purpose of disclosure is to allow OCSAR to match the personal information of ICAN FLO participants with data to be disclosed by South Australia Police (SAPOL) in order to conduct a statistical analysis of the impact of the ICAN FLO program on the offending behaviour of participants.

All other Principles continue to apply.

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

---

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

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is submitted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

Exemption – OCSAR (AGD)

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

This exemption applies for the study period 2006 to 2010 for the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information of participants in the Department for Education and Child Development (DECD) Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and were not enrolled in 2010. The information is to be collected and used by OCSAR for the purposes of evaluating the ICAN FLO program.

The personal information to be collected and used is:

- Name
- Date of Birth
- FLO enrolment dates
- Geographical are of school enrolment
- Whether the student is Aboriginal
- Whether the student had a disability
- Whether the student was under the Guardianship of the Minister

The purpose of collection and use is to allow OCSAR to match the personal information of ICAN FLO participants with data to be collected from South Australia Police (SAPOL) in order to conduct a statistical analysis of the impact of ICAN FLO on the offending behaviour of participants.

All other Principles continue to apply.

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

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is substituted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

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

This exemption applies for the study period 2006 to 2010 for the South Australia Police (SAPOL). It is an exemption from compliance with Principle 10, allowing SAPOL to disclose information held in the Police Incident Management System (PIMS) relating to participants in the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and not enrolled in 2010. The information is to be disclosed by SAPOL to the Office of Crime Statistics and Research (OCSAR) for the purposes of evaluating the ICAN FLO program.

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

The personal information to be disclosed is:

- Any police apprehensions occurring in the study period
- Any formal cautions occurring in the study period
- Any referrals to family conferences occurring in the study period
- The date of the offences
- The date of the report
- The number and type of charges listed (using JANCO offence codes)
- The Justice Information System (JIS) PIN for the student

The purpose of disclosure is to allow OCSAR to match the personal information of ICAN FLO participants with data held in the SAPOL PIMS database in order to conduct a statistical analysis of the impact of the ICAN FLO program on the offending behaviour of participants.

All other Principles continue to apply.

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is submitted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

Exemption – OCSAR (AGD)

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

This exemption applies for the study period 2006 to 2010 for the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use information held in South Australia Police's (SAPOL) Police Incident Management System (PIMS) relating to participants in the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and not enrolled in 2010. The information is to be collected and used by OCSAR for the purpose of evaluating the ICAN FLO program.

The personal information to be collected and used is:

- Any police apprehensions occurring in the study period
- Any formal cautions occurring in the study period
- Any referrals to family conferences occurring in the study period
- The date of the offences
- The date of the report
- The number and type of charges listed (using JANCO offence codes)
- The Justice Information System (JIS) PIN for the student

The purpose of collection and use is to allow OCSAR to match the personal information of ICAN FLO participants with data held in the SAPOL PIMS database in order to conduct a statistical analysis of the impact of the ICAN FLO program on the offending behaviour of participants.

All other Principles continue to apply.

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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

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

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

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is submitted to the Chief Executive of Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

Exemption – CAA

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

This exemption applies for the study period 2006 to 2010 for the Courts Administration Authority (CAA). It is an exemption from compliance with Principle 10, allowing CAA to disclose information from the CAA Court Outcomes Database relating to participants in the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and not enrolled in 2010. The information is to be disclosed to the Office of Crime Statistics and Research (OCSAR) for the purpose of evaluating the ICAN FLO program.

The personal information to be disclosed is:

- Any offences proven guilty during the period, including
    - Offence date
    - Date proven guilty
    - Number of charges proven guilty
    - Type of charges proven guilty
    - Penalties associated with any charges proven guilty

The purpose of disclosure is to allow OCSAR to match the Justice Information System (JIS) PIN of ICAN FLO participants with data to be collected from the CAA Court Outcomes Database for the purpose of conducting a statistical analysis of the impact of the ICAN FLO program on the offending behaviour of participants.

All other Principles continue to apply.

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

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is submitted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

Exemption – OCSAR (AGD)

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

This exemption applies for the study period 2006 to 2010 for the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use information from the Courts Administration Authority (CAA) Court Outcomes Database relating to participants in the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and not enrolled in 2010. The information is to be collected and used by OCSAR for the purpose of evaluating the ICAN FLO program.

The personal information to be collected and used is:

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

- Any offences proven guilty during the study period, including
    - Offence date
    - Date proven guilty
    - Number of charges proven guilty
    - Type of charges proven guilty
    - Penalties associated with any charges proven guilty

The purpose of collection and use is to allow OCSAR to match the Justice Information System (JIS) PIN of ICAN FLO participants with data to be disclosed by CAA from the Court Outcomes Database for the purpose of conducting a statistical analysis of the impact of the ICAN FLO program on the offending behaviour of participants.

All other Principles continue to apply.

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

Expiry

The exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is submitted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

Amended Exemption – DECD

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

This exemption applies for the study period 2006 to 2010 for the Department for Education and Child Development (DECD). It is an exemption from compliance with Principle 10, allowing DECD to disclose personal information of participants in the Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and were not enrolled in 2010. This exemption replaces the exemption issued on 7 August 2013. (Document reference D13/04714).

The personal information to be disclosed is:

- Name
- Date of Birth
- Gender
- FLO enrolment dates
- Geographical area of school enrolment
- Whether the student is Aboriginal
- Whether the student had a disability
- Whether the student was under the Guardianship of the Minister

The purpose of disclosure is to allow OCSAR to match the personal information of ICAN FLO participants with data to be disclosed by South Australia Police (SAPOL) in order to conduct a statistical analysis of the impact of the ICAN FLO program on the offending behaviour of participants.

All other Principles continue to apply.

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

---

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

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is submitted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

2 September 2013

Amended Exemption – OCSAR (AGD)

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

This exemption applies for the study period 2006 to 2010 for the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information of participants in the Department for Education and Child Development (DECD) Innovative Community Action Networks (ICAN) Flexible Learning Options (FLO) program who were enrolled in eight subsequent terms of FLO between 2007 and 2009 and were not enrolled in 2010. This exemption replaces the exemption issued on 7 August 2013. (Document reference D13/04715).

The personal information to be collected and used is:

- Name
- Date of Birth
- Gender
- FLO enrolment dates
- Geographical are of school enrolment
- Whether the student is Aboriginal
- Whether the student had a disability
- Whether the student was under the Guardianship of the Minister

The purpose of collection and use is to allow OCSAR to match the personal information of ICAN FLO participants with data to be collected from South Australia Police (SAPOL) in order to conduct a statistical analysis of the impact of ICAN FLO on the offending behaviour of participants.

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

All other Principles continue to apply.

Conditions

It is a condition of this exemption that ethics approval from the Families and Communities Research Ethics Committee for the OCSAR evaluation of the impact of the ICAN FLO program on participant offending behaviour remains current.

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 approved under the *State Records Act 1997*.

Expiry

This exemption will expire on the day the Final Report of the evaluation of the ICAN FLO program is substituted to the Chief Executive of the Department for Education and Child Development or on 17 April 2014, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

2 September 2013

APPENDIX D Exemptions Granted – Memorandum of Understanding to perform statistical monitoring, information analysis and dissemination

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[12] (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 the disclosure of personal information to the Office of Crime Statistics and Research (OCSAR) for that personal information to be used to perform a statistical monitoring, information analysis and dissemination role. Conditions apply.

All other Principles continue to apply.

Conditions

This authorisation for disclosure of personal information is conditional.

The personal information to be disclosed is described in the Memorandum of Understanding (MoU) between OCSAR and SAPOL. A synopsis of the MoU is available upon request. Broadly, it includes:

- extracts from SAPOL of unit record data from the Police Information Management System Incident and Apprehension databases;
- access to the SAPOL Offender History database; and
- access to the SAPOL General Enquiry Information System in the Justice Information System.

OCSAR has agreed to adhere to standards stipulated in the MoU with respect to the security and storage of data, and obtaining relevant ethics committee approval for research and evaluation projects (see separate exemption provided to OCSAR to enable it to collect the required personal information from SAPOL).

This exemption will apply during the period of operation of the MoU, and will cease to apply upon review and amendment or invalidation of the MoU. Continued application will be reviewed if the MoU is amended.

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*.

---

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

Expiry

This exemption expires five (5) years after approval, or upon review and amendment of the MoU, whichever is sooner. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

Exemption – OCSAR

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[13] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing the collection of personal information from South Australia Police (SAPOL), and use of that personal information to perform a statistical monitoring, information analysis and dissemination role that includes the:

- provision of statistical information to underpin reporting against South Australia's Strategic Plan targets;
- provision of statistical information to underpin targets set by other agencies;
- provision of statistical information to inform Parliamentary Committee Inquiries and Ministerial Taskforces;
- provision of an information service to both government and the public;
- statistical analysis of data in response to requests or self-initiated in response to a perceived need; and
- development and maintenance of a web based application called 'Crime Mapper' that allows users to access data on recorded offences by Local Government Area, Metropolitan SA, Regional SA and state-wide.

Conditions apply.

All other Principles continue to apply.

Conditions

This authorisation for collection and use of personal information is conditional.

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

The personal information to be disclosed is described in the Memorandum of Understanding (MoU) between OCSAR and SAPOL. A synopsis of the MoU is available upon request. Broadly, it includes:

- extracts from SAPOL of unit record data from the Police Information Management System Incident and Apprehension databases;
- access to the SAPOL Offender History database; and
- access to the SAPOL General Enquiry Information System in the Justice Information System.

The projects for which the personal information may be used must be consistent with the role and functions for which OCSAR was established, and must adhere to standards stipulated in the MoU with respect to the security and storage of data.

This exemption does not extend to any use of the data for research purposes. The use of data for research and evaluation projects will require a separate request for exemption and approval sought from the relevant ethics committee.

This exemption will apply during the period of operation of the MoU, and will cease to apply upon review and amendment or invalidation of the MoU. Continued application will be reviewed if the MoU is amended.

The data custodian, SAPOL, is willing and able to provide the data to OCSAR (see separate exemption provided to SAPOL to enable it to disclose the required personal information to OCSAR).

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 expires five (5) years after approval, or upon review and amendment of the MoU, whichever is sooner. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

7 August 2013

APPENDIX E Exemption Granted – SA NT DataLink – Cervix Screening Program

Exemption – SA Health

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[14] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to SA Health. It is an exemption from compliance with Principles 2, 8 and 10, allowing SA Health to disclose personal information to SA Health officers within the Data Linkage Unit of SA NT DataLink, and for that information to be collected and used for a purpose that was not the purpose of collection.

The personal information to be used is from SA Health's Cervix Screening Program and is limited to:

- Client identifier
- Date of screening
- Laboratory Assessment Number
- Names (all)
- Date of Birth
- Full address, including LGA codes
- Client deceased flag, "D".

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.

SA Health 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.

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 11 December 2013 to 10 December 2016. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

9 January 2014

APPENDIX F Exemptions Granted – Offender Management Plan Pilot Program

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

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[15] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), SA Health, Attorney-General's Department (AGD), Department of Further Education, Employment, Science and Technology (DFEEST), TAFE SA and the Department for Education and Child Development (DECD). It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, SA Health, AGD, DFEEST, TAFE SA and DECD to share case file information about the children of one selected offender, as agreed with the Committee, as part of the Offender Management Plan Pilot Program (OMP Pilot).

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

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

All other Principles continue to apply.

Conditions

This exemption is conditional on the personal information shared through the OMP Pilot only being used for the purposes of coordinated case management of the one particular serious offender and their children. It is also conditional on the individual offender being informed of their inclusion in the OMP Pilot.

This exemption is also conditional on the consent of one or both of the children's legal guardians being sought prior to the disclosure of the children's personal information. Only in circumstances where consent is not granted, or if it is given and then later revoked, does this exemption 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.

---

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

- Personal information is protected during transit; electronic information should be encrypted and password protected and physical files should not be left unattended in an unsecure environment.
- Access to personal information is on a strictly need-to-know basis. Personal information collected under the OMP Pilot should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under a participating offender's case management plan, delivering services to the offender as an existing client or where otherwise allowable under IPPs 8 and 10.

Destruction or retention of personal information

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

Expiry

This exemption applies from 14 May 2014 until 30 June 2015 or the end of the OMP Pilot, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
A/Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

5 June 2014

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

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[16] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), SA Health, Attorney-General's Department (AGD), Department of Further Education, Employment, Science and Technology (DFEEST) and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, SA Health, AGD, DFEEST and TAFE SA to share case file information of serious offenders as part of the Offender Management Plan Pilot Program (OMP Pilot).

The personal information to be shared is case file information and other personal information relevant to offenders included in the OMP Pilot. This includes the personal information of family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender. The information is collected and held by each agency through its mandated service provision.

The purpose of the collection, use and disclosure of the personal information is to allow the successful functioning of the OMP Pilot in providing coordinated case management of

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

selected serious offenders to reduce recidivism and promote community safety. This exemption also provides for the disclosure of relevant personal information to third party service providers necessary for the provision of targeted services to individual offenders under the OMP Pilot.

All other Principles continue to apply.

Conditions

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

This exemption is also conditional on consent being sought from family members and associates, where it has been identified that those individuals contribute significantly to the offending lifestyle of the nominated offender, for their personal information to be shared as part of the OMP Pilot. Only in circumstances where consent is not granted, or if it is given and then later revoked, does this exemption 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.
- Access to personal information is on a strictly need-to-know basis. Personal information collected under the OMP Pilot should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under a participating offender's case management plan, delivering services to the offender as an existing client or where otherwise allowable under IPPs 8 and 10.

Destruction or retention of personal information

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

Expiry

This exemption applies from 14 May 2014 until 30 June 2015 or the end of the OMP Pilot, whichever is earlier. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
A/Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

5 June 2014

APPENDIX G Exemption 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[17] (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.

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

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

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 16 June 2014 until 31 December 2014, 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

17 June 2014