Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2016

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

September 2016

For information and advice, please contact:

The Presiding Member
Privacy Committee of South Australia
c/- State Records of South Australia
GPO Box 464
ADELAIDE SA 5001

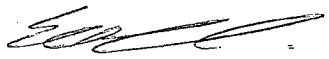
ph: (08) 8204 8786
fax: (08) 8204 8777
email: privacy@sa.gov.au

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

The Hon John Rau MP
ATTORNEY-GENERAL

Dear Attorney-General

The Privacy Committee of South Australia is pleased to provide you with this report of its activities for the year ending 30 June 2016. The report is provided pursuant to Clause 4A of the *Proclamation establishing the Privacy Committee of South Australia*, as amended and republished in the South Australian Government Gazette on 11 June 2009.



Simon Froude
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

30 September 2016

Table of Contents

1 Year in Review

During the reporting year, the Privacy Committee of South Australia (Privacy Committee) continued to provide advice and recommendations to the Minister and government agencies on the protection of privacy and the Information Privacy Principles Instruction (IPPI). It also continued to fulfil its role in receiving privacy complaints, responding to privacy enquiries, and granting exemptions from the IPPI that it considered in the public interest.

The Privacy Committee noted an increase in the number of exemptions from the IPPI extended or granted to State Government agencies in 2015-16. Many of these exemptions allowed for the sharing of personal information to enable more evidence based evaluation, monitoring and improved planning and analysis of government funded services and/or policy initiatives.

The Privacy Committee appreciates that access to government information and data can be of great benefit to Government, researchers and the community; however the collection, use and disclosure of personal information must always be balanced against an individual's right to privacy. In November 2015, the New South Wales Parliament passed the *Data Sharing (Government Sector) Act 2015* to promote and facilitate the expeditious sharing of government data to support policy making, program management and service planning and delivery. However this Act contains provisions to ensure that the sharing of health and other personal information complies with the requirements of the *Privacy and Personal Information Protection Act (NSW) 1998*.

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

This is a report of the activities of the Privacy Committee for the year ending 30 June 2016. 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

The IPPI can be accessed on the Department for the Premier and Cabinet website and in Appendix A of this report.

2.1.2 Amendments to the Information Privacy Principles Instruction

On 20 June 2016, Cabinet approved an amendment to the IPPI Schedule, pursuant to clause 2(3), to include the Compulsory Third Party Regulator (CTP Regulator) as an agency to which the IPPI does not apply. From 1 July 2016, certain personal information in relation to CTP policies will be handled by the CTP Regulator, rather than by the Motor Accident Commission (MAC). The MAC is an agency to which the IPPI does not apply. Accordingly, Cabinet deemed it appropriate that the CTP Regulator also be listed as an agency to which the IPPI does not apply.

The amendment comes into operation on 1 July 2016.

2.2 The Privacy Committee of South Australia

2.2.1 Establishment and Functions

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

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

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

2.2.2 Reporting

During 2015-16, 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 the membership of the Committee. It requires that the Committee consists of six members, all of whom are to be appointed by the Minister. Of the six members:

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

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

Presiding Member:

- Mr Simon Froude, Director, State Records of South Australia, Attorney-General's Department – appointed to 11 January 2017.

Members, in alphabetical order:

- Ms Kathy Ahwan, Principal Consultant, Policy and Legislation Unit, Department of Health and Ageing – appointed to 11 January 2017.
- Ms Deslie Billich, non-public sector employee – appointed to 30 September 2016.
- Mr Peter Fowler, Director, Security and Risk Assurance, Office for Digital Government, Department of the Premier and Cabinet – appointed to 30 June 2016.
- Ms Trish Simpson, Senior Solicitor, Out-posted, Crown Solicitor's Office, Attorney-General's Department – appointed to 22 February 2017.
- Ms Krystyna Slowinski, Senior Internal Auditor, Department for Communities and Social Inclusion – appointed to 2 June 2018.

Resignations

During the reporting year, Mr Peter Fowler tendered his resignation from the Privacy Committee.

Mr Fowler, Director, Security and Risk Assurance, Office for Digital Government, was appointed to the Committee in February 2014. Mr Fowler was appointed for his expertise in information technology, particularly in the area of information security. Mr Fowler's resignation is effective from 1 July 2016.

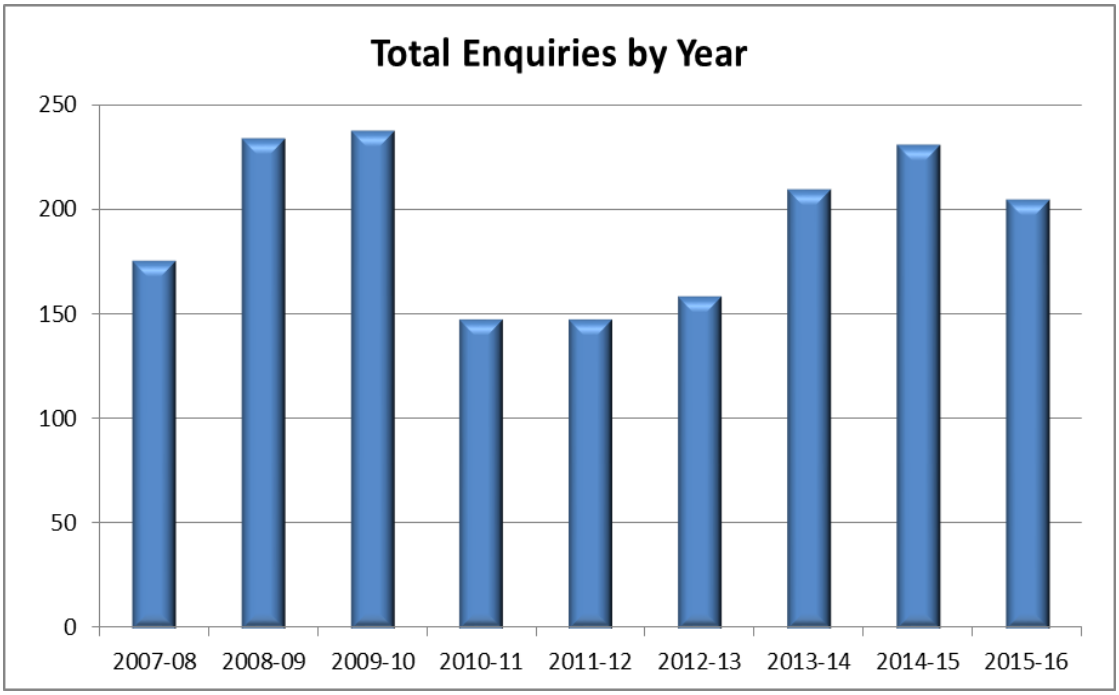
2.2.4 Resources

State Records of South Australia (State Records) provides executive support to the Privacy Committee including research and policy support, administrative support, meeting coordination, web hosting, and an enquiry and advice service to both agencies and the public. This resource includes the commitment of approximately one full time equivalent (FTE) staff. Due to resource constraints, the FTE committed to providing executive support was reduced to 0.5 FTE for most of 2015-16.

2.2.4.1 Privacy Enquiries

During the reporting year, State Records responded to 205 telephone and email enquiries from the public and State Government agencies relating to all aspects of privacy of personal information. This is 11 per cent less than the number of enquiries reported in 2014-15.

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



Over the reporting year:

- 69 per cent of all enquiries were dealt with over the telephone.
- The number of enquiries received from the public increased by 11 per cent from 94 in 2014-15 to 104 in 2015-16.
- The number of enquiries received from State Government agencies decreased by 26 per cent, from 137 in 2014-15 to 101 in 2015-16.
- Overall, 51 per cent of all enquiries received were from members of the public. This represents a slight shift from last year where the majority of enquires (57%) were received from State Government agencies.

2.2.4.2 Privacy Training

This year resourcing considerations have resulted in State Records being unable to deliver privacy training.

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 2015-16 totalled $64.38.

2.2.6 Meetings

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

2.2.7 Guidelines for members

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

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

2.2.8 South Australia's Strategic Plan

In 2011, the Government of South Australia published its second update to South Australia's Strategic Plan. The updated plan reflects the input and aspirations of communities for how to best grow and prosper and how South Australia can balance its economic, social and environmental aspirations in a way that improves overall wellbeing of the South Australian community, and creates even greater opportunities.

The activities of the Privacy Committee contribute to the achievement of Target 32 of South Australia's Strategic Plan. Target 32 'customer and client satisfaction with government services' is part of the broader goal of demonstrating strong leadership, working with and for the community within the 'Our Community' priority. The public expects a high degree of privacy protection when accessing government services, and also expects a degree of control over how their personal information will be collected, stored, used and disclosed.

The constitution of the Privacy Committee meets Target 30 (Priority: Our Community) to 'increase the number of women on all State Government boards and committees to 50% on average by 2014, and maintain thereafter by ensuring that 50% of women are appointed, on average, each quarter'. During the reporting year, the Privacy Committee maintained over 50% female membership.

2.2.9 Seven Strategic Priorities

In February 2012, the Premier announced the Government's seven strategic priorities. Those priorities are:

- creating a vibrant city;
- safe communities and healthy neighbourhoods;
- an affordable place to live;
- every chance for every child;
- growing advanced manufacturing;
- realising the benefits of the mining boom for all; and
- premium food and wine from our clean environment.

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

The work of the Privacy Committee supports the implementation of the priorities in relation to safe communities, healthy neighbourhoods, and every chance for every child. In particular, the Committee has provided exemptions relating to the Multi-Agency Protection Services Project, SA NT DataLink, and the Centre for Automotive Safety Research.

3 Activities of the Privacy Committee

3.1 Advice to the Minister

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

During the reporting year, the Privacy Committee continued to support the Minister and Government in the development of information privacy legislation for the South Australian public sector. The Committee remains concerned about the absence of a legislative framework for information privacy in the South Australian public sector.

In June 2016, State Records provided advice to the Minister regarding the *Health Care (Privacy and Confidentiality) Amendment Bill* introduced to the Legislative Council by the Hon. Stephen Wade M.L.C. The Bill seeks to amend the *Health Care Act 2008* to make it an offence for a health employee to improperly access or use health records or personal information.

3.2 Privacy Developments in other jurisdictions

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

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

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

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

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

3.2.1 Commonwealth, States and Territories

The Commonwealth and each State and Territory Government within Australia operate under varying legislative and administrative regimes for privacy protection, with the exception of Western Australia. These regimes are of interest to the Privacy Committee as it considers its own responses to local and national issues. Some of the significant developments in other jurisdictions are outlined below.

3.2.1.1 Australian Government

In its 2014 budget, the Australian Government announced its intention to abolish the Office of the Australian Information Commissioner (OAIC) through the introduction of the *Freedom of Information Amendment (New Arrangements) Bill 2014*.

The Bill stalled in the Senate and by April 2016 had lapsed at prorogation. The OAIC will continue to work with Australian businesses, agencies and individuals to deliver regulatory, public education and dispute resolution services in the areas of privacy, freedom of information and information management.

3.2.1.2 New South Wales

The *Data Sharing (Government Sector) Act 2015* was passed by the New South Wales (NSW) Parliament in November 2015 to remove barriers that impede the sharing of government sector data and to implement measures to facilitate the sharing of government sector data with the Data Analytics Centre and other agencies.

The legislation specifies safeguards in relation to the collection, use, disclosure, protection, keeping, retention or disposal of health information or personal information of individuals. The Bill was drafted in consultation with the NSW Privacy Commissioner. The sharing of personal data is excluded from the Act and is managed instead under the *Privacy and Personal Information Protection Act 1998*.

In March 2016, the NSW Legislative Council Standing Committee on Law and Justice recommended in its report *Remedies for the serious invasion of privacy in New South Wales* the establishment of a statutory cause of action for serious invasions of privacy. The Standing Committee went further to recommend a significant expansion of the powers of the NSW Privacy Commissioner to address claims of serious invasions of privacy.

The development of a statutory cause of action, as opposed to reliance on common law remedies, is supported by the NSW Privacy Commissioner and leading civil

rights, privacy, legal and academic groups across NSW and Australia. The NSW Government's response to the report is expected by 5 September 2016.

3.2.1.3 Victoria

In May 2016, the Victorian Government announced its plan to merge the Commissioner for Privacy and Data Protection and the Freedom of Information (FOI) Commissioner into a single office, streamlining Victoria's information and data oversight bodies.

A newly created Office of the Victorian Information Commissioner (OVIC) will look after freedom of information, privacy and data protection issues, matching similar New South Wales, Queensland and Commonwealth bodies.

It will be led by an Information Commissioner and will be supported by a Privacy and Data Protection Deputy Commissioner and a Public Access Deputy Commissioner.

3.2.1.4 Invitations from other jurisdictions

On 24 June 2015, the Presiding Member of the Committee received an invite from the Australian Government's Attorney-General's Department (AGD) to attend a national forum of Privacy Commissioners to discuss the privacy impacts of the central Interoperability Hub of the National Facial Biometric Matching Capability (Capability). The Capability will allow participating Commonwealth and State agencies to share and match facial images such as those used on identity documents like passports to achieve fraud detection, law enforcement, national security, service delivery, and community safety outcomes.

Although the Presiding Member was unable to attend the national forum, a copy of the Privacy Impact Assessment (PIA) and the AGD's draft response were provided to the Presiding Member for comment in September 2015. The following recommendations were specifically noted by the Privacy Committee:

> Recommendation 12
>
> State and territory representatives will be expected to consult with their respective privacy commissioners and/or ombudsmen in exercising their responsibilities for oversight of the Services.
>
> Recommendation 13
>
> … each jurisdiction accepting responsibility for resourcing of privacy regulators or other relevant bodies to oversight [sic] the participation of its agencies in the Services.

The Licensing, Transport Services Division in the Department for Planning, Transport and Infrastructure (DPTI) is the South Australian representative.

On 16 December 2015, the Presiding Member of the Privacy Committee was advised by email that the preliminary PIA had been released by the Australian Minister for Justice accompanied by the AGD's response which accepts all the PIA's recommendations, either in whole or in part. A copy of the Minister for Justice's media release and AGD response can be found at: https://www.ministerjustice.gov.au/Mediareleases.

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 four financial years.

In early December 2015, APPA delegates met in Macao for the 44th APPA Forum. The meeting which was hosted by the Office for Personal Data Protection, Macao, was attended by representatives from 13 privacy authorities. Delegates discussed emerging privacy issues from across the Asia Pacific region, including legal reforms and law enforcement issues, health information and biometrics, and various public education initiatives. Other matters discussed included public sector information sharing, telephony fraud involving personal data, privacy issues relating to electoral processes and political parties, the use of CCTV cameras by public security forces, and the implications of 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.

In January 2016, the Presiding Member of the Privacy Committee attended a PAA meeting. Some of the main issues discussed at the meeting included information sharing, combating domestic violence, security breaches, biometrics, and big data.

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 SA Health Workplace Surveillance Draft Policy

On 27 January 2016, the Committee received a copy of SA Health's draft policy entitled *Surveillance in and associated with the Workplace Policy Directive*. The policy covers the collection, use, storage and disclosure of overt and covert surveillance data in the workplaces of SA Health.

On 18 February 2016, the Committee provided feedback to SA Health on its draft policy including comments relating to the approval process, the need to refer to all

relevant legislation in the policy, and the Chief Executive's responsibility to comply with relevant legislation as well as the policy itself.

3.3.2 Office of the Technical Regulator – Access to Drainage Plans

In February 2016, the Office of the Technical Regulator (OTR) contacted the Privacy Committee to discuss providing electronic access to internal drainage plans to those who request them. Plumbers submit these plans when they have installed, replaced or altered sanitary drains within properties. These plans contain the homeowner's name and address which is arguably the personal information of the homeowner.

The Committee provided advice on whether the disclosure of these plans could be a breach of the IPPI and provided options for the OTR to consider. The OTR are seeking legal advice on how to proceed.

3.3.3 SA Health (Inspired SA)

On 1 February 2016, the Committee received a submission seeking an exemption from the IPPI to allow SA Health to disclose to researchers at Flinders University data regarding hospitalisation and emergency department utilisation for a cohort of residents living in residential aged care facilities who have cognitive impairment. This cohort of residents previously participated in the INSPIRED (SA) study. INSPIRED (SA) is a cross-sectional, observational pilot study to evaluate the specialised dementia services currently being provided at residential aged care facilities in South Australia.

At its meeting on 17 February 2016, it was agreed that the Privacy Committee did not have the authority to provide an exemption as this type of disclosure must be authorised under section 93 of the *Health Care Act 2008* or section 106 of the *Mental Health Act 2009* (whichever is relevant).

3.3.4 Australian Bureau of Statistics – 2016 Census

On 11 November 2015, the Presiding Member of the Privacy Committee was advised by the Australian Bureau of Statistics (ABS) of its intention to conduct a privacy impact assessment (PIA) on the proposed retention of names and addresses from responses to the 2016 Census of Population and Housing.

Historically the ABS has destroyed all names and addresses after statistical processing of the Census is complete, however the ABS claimed that retaining the names and addresses would provide a benefit to the ABS and wider community by enabling higher quality linkage of datasets, supporting organisational efficiencies such as the development of an address register, and supporting more flexible geospatial outputs.

On 18 December 2015, the Committee was advised that after consideration of a the completed PIA, focus group testing, and feedback from Privacy and Information Commissioners, the ABS made the decision to retain names and addresses from the 2016 Census.

The ABS advised that the PIA assessed the level of risk to personal privacy, considering the protections in place, as very low. The ABS is confident that the risks identified are effectively mitigated by storing names and addresses separately from other Census data as well as separately from each other. The risks are further mitigated by governance and security arrangements the ABS already has in place.

The retention of names and addresses collected in the 2016 Census is consistent with the functions of the ABS prescribed in the *Australian Bureau of Statistics Act 1975* and compliant with all the provisions in the *Census and Statistics Act 1905* and the *Privacy Act 1988*, including the Australian Privacy Principles.

The Presiding Member of the Committee met with members of the ABS on 7 April 2016 and agreed to publish on the State Records website an information sheet outlining how the ABS protect privacy in the Census. As at 30 June 2016, no complaints had been received by the Privacy Committee regarding the census.

3.3.5 SA Health Privacy Policy Directive

On 29 September 2015, the Presiding Member of the Privacy Committee received an email from SA Health advising that the *Code of Fair Information Practice* had been reviewed and a new policy developed to ensure that the information provided around privacy reflects legislative and other policy requirements that currently apply within South Australia. A copy of the draft Privacy Policy Directive was provided to the Committee for comment.

The Privacy Committee responded to SA Health suggesting minor amendments to some of the wording in the draft policy.

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.

3.4.1 Guidelines and Information Sheets

There were no new privacy guidelines or information sheets developed during the 2015-16 reporting year.

3.4.2 Participation in committees and groups

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

- South Australian Government's ICT Security and Risk Steering Committee
- Security Managers Round Table
- Cyber Taskforce
- National Identity Security Coordination Group

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

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

The Privacy Committee seeks reports from agencies from time to time on their compliance with the IPPI and, in some cases, this is a condition of an exemption. In addition, under the terms of the IPPI, the Privacy Committee may on its own initiative appoint a person to investigate or assist in the investigation of the nature and extent of compliance with the IPPI.

3.5.1 Privacy Breaches

3.5.1.1 Northern Adelaide Local Health Network

On 29 July 2015, the Northern Adelaide Local Health Network (NALHN) advised State Records there had been a breach of patient confidentiality at the Lyell McEwin Hospital.

The breach involved a midwife who had misplaced documents concerning antenatal and postnatal women. The documents detailed names, addresses, phone numbers, pathology results, generic education information and blank referral forms. It also included student midwife names and their phone numbers. A member of the public found the documents and advised NALHN on 26 July 2015. Staff at the Lyell McEwin Hospital contacted all of the women whose details were contained within the documents to advise them of the incident.

Consistent with the requirements of the *State Records Act 1997*, State Records undertook a survey of the recordkeeping practices of NAHLN in relation to the incident. The investigation highlighted that NAHLN had made the necessary changes to improve their records management practices after the incident occurred. The results of the investigation will be provided to the Privacy Committee for consideration.

3.5.1.2 SACE Board

On 15 December 2015, the SACE Board (the Board) released year 12 student results online. Due to a technical fault, when logging into the Students Online system some students were provided with another student's tertiary entrance statement or 'dummy data' of a pretend student. The issue was investigated and resolved by the Board's information systems staff within half an hour.

The Board advised the Privacy Committee of the incident on 17 December 2015. The Board acknowledged that this was a breach of the IPPI and advised that the Board was investigating the exact cause of the system fault.

In February 2016, the Committee considered the privacy breach and sought an update from the Board. On 24 March 2016, the Board provided an update on the technical cause of the problem and the solution, as well as what measures had been considered, or taken, to ensure the online system does not breach the privacy of students in the future, such as conducting audits, improving the Students Online system, and investigating other products and technologies. The Committee asked

that the Board provide an additional report at the end of 2016 once the students' results are released, addressing how the system performed.

3.5.1.3 SA Health

In late February 2016, a number of media articles reported that 21 staff had inappropriately accessed patient records in the past year.

The various articles stated that SA Health conducted an audit which discovered that in the past year, 13 staff had accessed the medical records of a particular patient and that a further eight staff had accessed medical records of other patients without the proper authority. The articles stated that an internal investigation was undertaken by SA Health leading to either the counselling of staff involved, disciplinary action, or in the case of two staff, termination of employment.

On 29 February 2016, the Privacy Committee wrote to the Chief Executive of SA Health and requested a copy of the audit results, a copy of the SA Health's internal investigation report, and an explanation as to what steps have or will be taken by SA Health to prevent unauthorised access to patient records in the future.

A response was provided by SA Health on 21 March 2016 advising that due to having to finalise a number of its own internal inquiries, a targeted response would be provided to the Committee at a future date.

3.5.1.4 South Australia Police

By letter dated 9 June 2016, South Australia Police (SAPOL) advised the Privacy Committee of an agreement between itself and the Equal Opportunity Commission (EOC) for the EOC to conduct a survey of current and former SAPOL employees as part of its review into sex discrimination, sexual harassment, and predatory behaviour. In order for the EOC to survey former or inactive employees, SAPOL disclosed to the EOC the names and contact details of several employees no longer employed by SAPOL so that the EOC could approach these people directly and invite each to participate in the survey.

A query was received by the EOC regarding a potential breach of the IPPI. In light of this, SAPOL requested the EOC to expunge from their records any personal information relating to former SAPOL employees sourced during the process.

SAPOL and the EOC have temporarily halted all information exchange to allow all processes to be assessed to ensure IPPI compliance. Any further personal information required by the EOC will be obtained by consent.

The Committee was satisfied that the action taken by SAPOL to address the breach was sufficient and that no further action was required.

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 Privacy Committee may also refer the complainant to the South Australian Ombudsman if it remains dissatisfied with the agency's response.

If the complaint relates to privacy breaches in the delivery of Government health services, the Committee may refer the complaint to the Health and Community Services Complaints Commissioner. If the complaint relates to privacy breaches in relation to the South Australia Police, the Committee may refer the complaint to the Police Ombudsman. The Committee may also refer matters to the Independent Commission Against Corruption, via the Office for Public Integrity, should it consider a matter to fall within its jurisdiction of misconduct or maladministration.

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

Three formal complaints were received during the reporting year. One was concluded, one withdrawn, and the other postponed. One complaint received in the previous financial year was also concluded.

3.6.1 Complaints Concluded in 2015-16 – Summary Table

	Respondent Organisation	Information Privacy Principle (IPP)	Outcome
1	Government Department	IPP 10 – Disclosure of personal information to third party	Concluded
2	Government Department	IPP 4 – Storage of Personal Information IPP 8 – Use 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 Privacy Committee considers that the public interest for an activity outweighs the privacy protections afforded by the IPPI, or where otherwise warranted by unique circumstances. Exemptions are generally subject to conditions, such as an expiry date, an approval from an appropriate research ethics committee, or a requirement for the agency to report on the activity conducted under the exemption.

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

3.7.1 Multi-Agency Protection Services Project

In October 2015 and May 2016, the Privacy Committee considered requests from SAPOL seeking extensions to its exemption from the IPPI 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 between a number of agencies to protect victims, or potential victims, of domestic violence and/or child protection referrals.

On 7 October 2015, representatives from SAPOL met with the Privacy Committee and provided some background information about MAPS and addressed issues around the sharing of personal information with participating agencies and the future of the MAPS program. The Committee agreed to grant a further extension to its exemption due to the significant nature of the work undertaken by the MAPS Project. The exemption was extended to 30 June 2016.

In May 2016, the Committee agreed to grant SAPOL and all participating agencies a further 12 month extension to its exemption to allow MAPS to continue to operate effectively while the future of the project is further considered by SAPOL.

See Appendix C for the full text of the exemptions.

3.7.2 Offender Management Plan Program

In July 2015, the Privacy Committee considered a submission from SAPOL seeking a 12 month extension to its exemption from the IPPI for the Offender Management Plans (OMP) Program.

Due to concerns surrounding the security of personal information provided to the OMP Program by participating agencies and issues with consent, the Privacy Committee determined to grant an interim three month extension on the condition that representatives from the OMP Program attended the next Committee meeting to address the concerns.

On 17 September 2015, representatives from the OMP Program attended an extraordinary Committee meeting. Representatives were able to satisfy the Privacy Committee that the issues surrounding consent and security were being dealt with. During the meeting, the Committee suggested amendments to the OMP Pilot Practice Guidelines.

Considering the steps taken by SAPOL to address issues with security and consent, the Privacy Committee agreed to grant a further nine month extension to its exemption from the IPPI, which expired on 30 June 2016.

In May 2016, the Privacy Committee considered a further submission from SAPOL to extend the exemption. Due to certain concerns, including concerns around the ongoing nature of the OMP Program, the Committee determined to grant an interim four month extension and requested that representatives from the OMP Program attend an upcoming meeting to address specific questions around consent, the level of information provided to participants in the program, and the purpose for which the information collected will be used.

See Appendix D for the full text of the exemptions.

3.7.3 Centre for Automotive Safety Research

In July 2015, the Privacy Committee considered a request from SAPOL to broaden its existing exemption from the IPPI so it could provide the Centre for Automotive Safety Research (CASR) with a range of personal information of crash participants, including addresses. The Committee agreed to grant a broader exemption on the conditions that letters sent to individuals asking for their consent explain how CASR came to be in possession of their address and other personal information, and that CASR maintains research ethics approvals from SA Health and the University of Adelaide.

In March 2016, the Privacy Committee considered a request from SAPOL for an interim extension to its exemption to allow SAPOL to finalise and approve a submission seeking a longer term extension. The Committee considered this request at its meeting on 17 February 2016 and agreed to grant a three month interim extension until 18 May 2016.

In April 2016, the Privacy Committee received a submission requesting an extension of 12 months. The Committee determined to grant an interim exemption of two months. Before considering a longer extension, the Committee requested further information from SAPOL which was provided by letter dated 21 June 2016.

At its meeting on 29 June 2016, the Privacy Committee considered SAPOL's response. Based on the information provided, members agreed to grant a further 12 month extension for SAPOL to continue to provide personal information of crash participants contained within Vehicle Collision Reports to CASR.

See Appendix E for the full text of the exemptions.

3.7.4 Aspire Adelaide Program and Ruby's Reunification Program

In November 2015, the Privacy Committee considered a submission from the Department for Communities and Social Inclusion (DCSI) seeking exemptions from the IPPI for multiple agencies to allow for data matching of certain individuals associated with the Aspire Adelaide Program for the development of a Homelessness Social Impact Bond.

Due to the need for the Department of the Premier and Cabinet (DPC), the coordinating agency, to negotiate and develop the Social Impact Bond promptly, the submission was considered by the Privacy Committee out of session. In November 2015, a quorum of the Committee agreed to grant a 12 month exemption to all participating agencies to share information about homeless individuals associated with the Aspire Adelaide Program.

The Privacy Committee further discussed this request for an exemption at its meeting on 25 November 2015. The Committee raised some questions around whether the disclosure of information by participating agencies was a 'one-off', what would happen with the identifiable data once the linkage process had been completed, and in what form the data would be reported to DPC, the co-ordinating agency.

On 23 June 2016, the Committee received a submission from DPC seeking a 12 month exemption from the IPPI to allow personal information of clients of the Ruby's Reunification Program, contained in a database managed by DCSI, to be disclosed to Families SA to allow Families SA to undertake data matching and analysis.

Ruby's Reunification Program is currently funded through DCSI as a homeless prevention program targeting young people aged between 12-17 years.

At its meeting on 29 June 2016, the Committee agreed to grant both DCSI and Families SA 12 month exemptions to disclose and use personal information regarding clients of the Ruby's program.

The Committee also brought to the attention of DPC that it had yet to answer questions from the Privacy Committee in relation to the Aspire Adelaide Program. A response was received by DPC on 21 July 2016 and is yet to be considered by the Committee.

See Appendix F for the full text of the exemptions.

3.7.5 SA NT DataLink – Multiple Exemptions

On 30 September 2015, SA NT DataLink requested extensions to 13 exemptions from the IPPI previously issued by the Privacy Committee, for a period of five years. Below is a list of the datasets for which extensions were requested:

- SA Public Hospitals Separations
- SA Public Hospital Emergency Department Presentations
- SA Cancer Registry
- Women's and Children's Health Network Data
- SA Health Perinatal Data
- SA Dental Services Data
- SA Health Cervical Cancer Data
- SA Public Schools Enrolments Census
- DECD – Families SA (Alternative Care, Care and Protection Orders and Child Protection)
- Youth Justice Data
- Housing SA Data
- SA Births and Deaths Registries
- SA Electoral Roll

The Privacy Committee considered the request at its meeting on 25 November 2015. The Committee noted that SA NT DataLink's current Joint Venture Consortium Agreement (JVA) would expire on 31 December 2015 and that SA NT DataLink is in the process of extending the JVA for a further five year period and expects to have the agreement in place by 1 January 2016. The Committee further noted that the scope of the datasets had not changed in any significant way.

The Privacy Committee agreed to extend the 13 exemptions to 31 December 2020 on the condition that a current JVA is in place by 1 January 2016. SA NT DataLink advised in March 2016 that the new JVA was in place as at 1 January 2016.

See Appendix G for the full text of the exemptions.

Appendices

APPENDIX A Information Privacy Principles

CABINET ADMINISTRATIVE INSTRUCTION 1/89, ALSO KNOWN AS THE INFORMATION PRIVACY PRINCIPLES (IPPS) INSTRUCTION, AND PREMIER AND CABINET CIRCULAR 12, AS AMENDED BY CABINET 20 JUNE 2016

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, 16 September 2013 and 20 June 2016)

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 1 July 2016.

(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)

Compulsory Third Party Regulator

Office for Public Integrity

South Australian Asset Management Corporation

WorkCover Corporation of South Australia

APPENDIX B Proclamation of the Privacy Committee of South Australia

Version: 11.6.2009

South Australia

Privacy Committee of South Australia

1—Establishment and procedures of Privacy Committee of South Australia

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

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

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

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

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

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

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

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

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

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

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

(a) dies;

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

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

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

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

(ii) neglect of duty;

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

(iv) misconduct.

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

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

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

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

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

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

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

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

2—Functions of the Committee

The Committee will have the following functions:

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

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

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

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

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

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

3—Prohibition against disclosure of information

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

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

(b) as required or authorized by law.

4—Exemptions

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

4A—Annual report

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

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

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

5—Interpretation

In this proclamation, unless the contrary intention appears—

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

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

APPENDIX C Exemptions Granted – Multi-Agency Protection Services Project

Exemption – SAPOL, DCS, SA Health, DCSI, DECD

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[1] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), SA Health, Department for Communities and Social Inclusion (DCSI) including the Office for Women, and Department for Education and Child Development (DECD) including Families SA. It is an exemption from compliance with IPPs 2, 7, 8 and 10, allowing SAPOL, DCS, SA Health, DCSI and DECD to share information and intelligence as part of SAPOL's Multi-Agency Protection Services (MAPS) Project. This exemption follows on from the previous interim exemption expiring on 31 December 2015 (D15/01910).

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

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

All other Principles continue to apply.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices. Participating agencies must specifically ensure that:

- Steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse.
- Personal information is kept in a secure area within participating agencies.
- Personal information is protected during transit; electronic information should be encrypted and password protected; and physical files should not be left unattended in an unsecure environment.
- Personal information collected under the MAPS Project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the MAPS Project, or

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

when delivering services to an individual as an existing client or where otherwise allowable under IPPs 8 and 10.

Destruction or retention of personal information

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

Expiry

This exemption applies from 1 January 2016 until 30 June 2016, or the end of the MAPS Project, whichever is earlier.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
23 October 2015

Exemption – SAPOL, DCS, SA Health, DCSI, DECD

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

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), SA Health, Department for Communities and Social Inclusion (DCSI) including the Office for Women, and Department for Education and Child Development (DECD) including Families SA. It is an exemption from compliance with IPPs 2, 7, 8 and 10, allowing SAPOL, DCS, SA Health, DCSI and DECD to share information and intelligence as part of SAPOL's Multi-Agency Protection Services (MAPS) Project. This exemption follows on from the previous interim exemption expiring on 31 December 2015 (D15/01910).

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

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

All other Principles continue to apply.

Security of Personal Information

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

security management systems and practices. Participating agencies must specifically ensure that:

- Steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse.
- Personal information is kept in a secure area within participating agencies.
- Personal information is protected during transit; electronic information should be encrypted and password protected; and physical files should not be left unattended in an unsecure environment.
- Personal information collected under the MAPS Project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the MAPS Project, or when delivering services to an individual as an existing client or where otherwise allowable under IPPs 8 and 10.

Destruction or retention of personal information

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

Expiry

This exemption applies from 1 July 2016 until 30 June 2017, or the end of the MAPS Project, whichever is earlier.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
27 May 2016

APPENDIX D Exemptions Granted – Offender Management Plan

Exemption – SAPOL, DCS, DCSI, SA Health, AGD, DSD, TAFE SA

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

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), SA Health, Attorney-General's Department (AGD), Department of State Development (DSD), and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, SA Health, AGD, DSD, 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 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 following:

- personal information shared through the OMP Pilot is only used for the purposes of coordinated case management of selected serious offenders;
- individual offenders are informed of their inclusion in the OMP Pilot;
- consent is 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; and
- prior to the expiry of this exemption, SAPOL arrange for representatives of the OMP Pilot to attend a Committee meeting to discuss concerns raised by the Committee at its meeting held on 8 July 2015.

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 1 July 2015 until 30 September 2015 or the end of the OMP Pilot, whichever is earlier. An extension may be considered by the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
27 July 2015

Exemption – SAPOL, DCS, DCSI, SA Health, AGD, DSD, TAFE SA

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

This exemption applies to the South Australia Police (SAPOL), Department for Correctional Services (DCS), Department for Communities and Social Inclusion (DCSI), SA Health, Attorney-General's Department (AGD), Department of State Development (DSD), and TAFE SA. It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DCSI, SA Health, AGD, DSD, 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 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 following:

- personal information shared through the OMP Pilot is only used for the purposes of coordinated case management of selected serious offenders;
- individual offenders are informed of their inclusion in the OMP Pilot; and
- consent is 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 1 October 2015 until 30 June 2016 or the end of the OMP Pilot, whichever is earlier. An extension may be considered by the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
24 September 2015

APPENDIX E Exemptions Granted – Centre for Automotive Safety Research

Revised Exemption – SAPOL

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

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

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

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

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

All other Principles continue to apply.

Conditions

This revised exemption is granted on the following conditions:

- information disclosed to CASR is only to be used by CASR for the purpose of obtaining further information relevant to the research being undertaken and for contacting persons involved in vehicle collisions to gain their consent to be interviewed;
- the letter sent to persons involved in vehicle collisions for the purpose of gaining their consent explains how CASR came to be in possession of their address and other personal information; and
- CASR maintains current research ethics approvals from the University of Adelaide and SA Health.

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

Security

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

Destruction or retention of personal information

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

Expiry

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

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
27 July 2015

Exemption – SAPOL

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

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

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

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

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

All other Principles continue to apply.

Conditions

This interim exemption is granted on the following conditions:

- information disclosed to CASR is only to be used by CASR for the purpose of obtaining further information relevant to the research being undertaken and for contacting persons involved in vehicle collisions to gain their consent to be interviewed;
- the letter sent to persons involved in vehicle collisions for the purpose of gaining their consent explains how CASR came to be in possession of their address and other personal information; and
- CASR maintains current research ethics approvals from the University of Adelaide and SA Health.

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

Security

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

Destruction or retention of personal information

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

Expiry

This interim exemption applies from 19 February 2016 to 18 May 2016. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
9 March 2016

Exemption – SAPOL

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

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

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

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

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

All other Principles continue to apply.

Conditions

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

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

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 18 May 2016 to 18 July 2016.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
2 June 2016

Exemption – SAPOL

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

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

The personal information to be disclosed by SAPOL to CASR relates to the personal information of persons involved in vehicle collisions contained within the Vehicle Collision Report. This information includes:

- Family and given names
- Address
- Gender
- Date of birth
- Age
- Licence number and State
- Licence status
- Phone numbers
- Seatbelt status
- Helmet status
- Hospital

- Injury level
- Breath analysis result
- BAC level
- Vehicle registration number
- Vehicle year and make

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

All other Principles continue to apply.

Conditions

This exemption is granted on the following conditions:

- information disclosed to CASR is only to be used by CASR for the purpose of obtaining further information relevant to the research being undertaken and for contacting persons involved in vehicle collisions to gain their consent to be interviewed;
- the letter sent to persons involved in vehicle collisions for the purpose of gaining their consent explains how CASR came to be in possession of their address and other personal information; and
- CASR maintains current research ethics approvals from the University of Adelaide and SA Health.

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

Security

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

Destruction or retention of personal information

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

Expiry

This exemption applies from 19 July 2016 to 18 July 2017. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
7 July 2016

APPENDIX F Exemptions Granted – Aspire Adelaide Program and Ruby's Reunification Program

Exemption – DCSI, AGD, SAPOL, SA Health, DCS and 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 (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Communities and Social Inclusion (DCSI), Office of Crime Statistics and Research (OSCAR) which is part of the Attorney-General's Department, South Australia Police (SAPOL), SA Health, Department for Correctional Services (DCS), and the Courts Administration Authority (CAA). It is an exemption from compliance with IPP 10, allowing DCSI, OSCAR, SAPOL, and CAA to disclose information, and from IPP 2 and 8 allowing OSCAR, SA Health, and DCS to collect and use information, as part of the social impact bond data matching project (project) led by the Department of the Premier and Cabinet.

The personal information to be disclosed includes:

- DCSI disclosing identifiable data from the H2H Homelessness Database to OSCAR and SA Health for individuals who meet the criteria for entry into the Aspire Adelaide Program. Identifiable personal information being disclosed includes: name, date of birth, gender, Aboriginality and/or Torres Strait Islander indicator, complexity indicator, length of support period, and country of birth. Data will not be provided for people whose records are tagged 'locked' or 'sensitive' in the H2H system.
- SAPOL disclosing to OSCAR information about any apprehensions during the study period, including offence date, report date, number and types of charges listed, and Justice Information Systems (JIS) PINs.
- CAA disclosing to OSCAR any convictions for offences committed during the study period, including offence date, date proven guilty, and the number and type of charges proven guilty.
- OSCAR disclosing to DCS a list of JIS PINs.

The personal information to be collected and used includes:

- DCS collecting and using matched JIS PINs from OSCAR.
- OSCAR collecting and using identifiable data of homeless individuals within the justice system from DCSI, SAPOL, DCS and CAA.
- SA Health collecting and using identifiable data of homeless individuals within the health system from DCSI.

The personal information to be collected, used and disclosed is held by one or more agencies through normal and accepted business processes.

The purpose of the collection, use and disclosure of the personal information is to allow for data matching across government agencies to gain an understanding of the use of state government funded health, justice and homelessness services of individuals included in the study compared to the general population. This will

enable the government to develop a social impact bond with relevant bodies, such as the Hutt Street Centre, to address homelessness in South Australia.

All other Principles continue to apply.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices. Participating agencies must specifically ensure that:

- Steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse.
- Personal information is kept in a secure area.
- Personal information is protected during transit and physical files should not be left unattended in an unsecure environment.
- Personal information collected as part of the project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the project.

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 18 November 2015 until 17 November 2016, or the end of the project, whichever is earlier.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – DCSI, DECD (Families 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 (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Communities and Social Inclusion (DCSI) and Families SA. It is an exemption from compliance with IPP 10, allowing DCSI to disclose information to Families SA, and from IPPs 2 and 8 allowing Families SA to collect and use information.

The personal information to be disclosed by DCSI includes the names, dates of birth, gender, and address of clients of the Rubys Reunification Program (aged between 12 and 17 years) as recorded in the H2H Homelessness Database.

The personal information of Rubys clients will be collected by Families SA and matched to data in the C3MS database. Families SA staff will analyse this information and provide the results of the analysis to the Department of the Premier and Cabinet. The results will not contain any identifiable personal information.

The purpose of the collection, use and disclosure of the personal information is to understand the profile of Rubys clients and the patterns of their involvement with the child protection system in order to investigate the feasibility of using social impact investment to expand the Rubys program.

The personal information to be collected, used and disclosed is held by agencies through normal and accepted business processes.

All other Principles continue to apply.

Security of Personal Information

The security of the personal information should be managed in line with the Government's Protective Security Management Framework (Premier and Cabinet Circular 30) and Information Security Management Framework, and the agency's security management systems and practices. Participating agencies must specifically ensure that:

- Steps taken to secure personal information are proportionate to its sensitivity and the risk of its loss or misuse.
- Personal information is kept in a secure area.
- Personal information is protected during transit and physical files should not be left unattended in an unsecure environment.
- Personal information collected as part of the project should not be on-disclosed or distributed further within participating agencies for any purposes other than facilitating any actions under the project.

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

These exemptions apply from 29 June 2016 until 28 June 2017, or the end of the project, whichever is earlier.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
7 July 2016

APPENDIX G Exemptions Granted – SA NT DataLink and Various Agencies

Exemption – SA Health (Morbidity and Emergency Department Dataset)

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

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

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

- Personal Information
  - Personal Identifier
  - Names – all names including nicknames, aliases and aka
  - Date of birth
  - Sex
  - Title
  - Aboriginality, Torres Strait Islander Indicator
  - Country of birth
  - Full address
- Event information
  - Dates of admission and discharge

All other Principles continue to apply.

Conditions

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Morbidity and Emergency Department Dataset)

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

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

The personal information to be used is from SA Health's public hospital inpatients morbidity dataset and the emergency department dataset and is limited to:

- Personal Information
  - Personal Identifier
  - Names – all names including nicknames, aliases and aka
  - Date of birth
  - Sex
  - Title
  - Aboriginality, Torres Strait Islander Indicator
  - Country of birth
  - Full address
- Event information
  - Dates of admission and discharge

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of master linkage keys in the establishment 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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 1 January 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Cancer Registry)

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

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

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

- Personal Identifier
- Names – all names including nicknames, aliases and aka
- Date of birth
- Date of death
- Sex
- Title
- Aboriginality, Torres Strait Islander Indicator
- Country of birth
- Full address including geocodes if available
- Any of the above information provided for other family members and included in these records.

All other Principles continue to apply.

Conditions

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Child, Youth and Women's Health Service Dataset)

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

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

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

- Unique record identifier
- Unique person identifier where available
- Names
- Date of birth
- Birth weight
- Sex
- Title

- Aboriginality, Torres Strait Islander indicator
- Country of birth
- Full address including geocodes if available
- Any of the above information provided for other family members and included in these records.

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of Master Linkage Keys in the 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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 1 January 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Perinatal Dataset)

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

This exemption applies to the Department for Health and Ageing (SA Health). It is an exemption from compliance with Principles 8 and 10, allowing SA Health to use

personal information for a purpose that was not the purpose of the collection of that information and to disclose that information to SA NT DataLink.

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

Mother and baby variables

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

Additional variables

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

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of Master Linkage Keys in the 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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 1 January 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Dental Dataset)

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

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

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

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

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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 1 January 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Cervix Screening Program)

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

This exemption applies to SA 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.

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 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – DECD (Public School Enrolment Dataset)

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

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

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

- Record Identifier
- Personal Identifier
- Names

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

All other Principles continue to apply.

Conditions

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

DECD remains responsible for the secure transfer of personal information in line with the IPPs.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Public School Enrolment Dataset)

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

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

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

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

All other Principles continue to apply.

Conditions

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – DECD (Families SA Dataset)

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

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

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

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

All other Principles continue to apply.

Conditions

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

DECD remains responsible for the secure transfer of personal information in line with the IPPs.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Families SA Dataset)

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

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

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

- Record identifier
- Names – all names including nicknames, aliases and aka
- Date of birth
- Sex
- Aboriginality, Torres Strait Islander indicator
- Cultural group
- Full address including geocodes where available

- Client File Number (85 File Number for Client Information System (CIS) records within the Justice Information System (JIS) – a flag indicating that this child was under the Guardianship of the Minister)
- Any of the above information provided for other family members and included in these records, i.e. full name and date of birth of the mother and father of the child or young person.

All other Principles continue to apply.

Conditions

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

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 12 December 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – DCSI (Youth Justice Dataset)

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

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

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

- Unique record identifier (i.e. episode reference number)
- Unique person identifier where available
- Given name(s) (including all ‘akas’, aliases and nicknames)

- Date of birth and country of birth
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Full address including geocodes where available
- The full name and date of birth of the mother and father of the child or young person where available.

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of Master Linkage Keys in the further development of the Master Linkage File as part of the SA NT Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of SA Health within the Data Linkage Unit.

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 19 February 2018 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA NT DataLink (Youth Justice Dataset)

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of

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

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

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

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

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of Master Linkage Keys in the further development of the Master Linkage File as part of the SA NT Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of SA Health within the Data Linkage Unit.

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 19 February 2018 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Housing SA Dataset)

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

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

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

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

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

All other Principles continue to apply.

Conditions

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 25 November 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – DCSI Housing SA (Housing SA Dataset)

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

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

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

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

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

All other Principles continue to apply.

Conditions

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

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

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 25 November 2015 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Births and Deaths Dataset)

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

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

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

Death Dataset

- Unique record identifier (registration number)
- Names (all names where available including surnames, surnames at birth, given names and given names at birth)
- Date of birth
- Date of death
- Age at death

- Place of birth
- Place of death
- Sex
- Aboriginality and/or Torres Strait Islander indicator
- Full residential address, including geocodes, where available.

Birth Dataset

The following personal information to be used from the births dataset is limited to birth records created after 1/1/1990.

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

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

All other Principles continue to apply.

Conditions

The information is only to be used 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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 1 January 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – AGD OCBA (Births and Deaths Dataset)

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

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

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

Death Dataset

- Unique record identifier (registration number)
- Names (all names where available including surnames, surnames at birth, given names and given names at birth)
- Date of birth
- Date of death
- Age at death
- Place of birth
- Place of death
- Sex

- Aboriginality and/or Torres Strait Islander indicator
- Full residential address, including geocodes, where available.

Birth Dataset

The following personal information to be used from the births dataset is limited to birth records created after 1/1/1990.

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

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

All other Principles continue to apply.

Conditions

The information is only to be used 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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

Security

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

Destruction or retention of personal information

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

Expiry

This exemption is granted from 1 January 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – SA Health (Electoral Roll Dataset)

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

This exemption applies to the Department for Health and Ageing (SA Health). It is an exemption from compliance with Principles 2 and 8, allowing SA Health to collect and use personal information for a purpose that was not the purpose of the collection of that information.

The personal information to be used is from the Electoral Commission of South Australia's South Australian Electoral Roll Dataset and is limited to:

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

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of Master Linkage Keys in the further development of the Master Linkage File as part of the SA NT Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of 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.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 21 February 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015

Exemption – ECSA (Electoral Roll Dataset)

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

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

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

- Elector Number
- Title
- Family Name
- Given Names

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

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

All other Principles continue to apply.

Conditions

The information is only to be used for the creation of Master Linkage Keys in the further development of the Master Linkage File as part of the SA NT Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of SA Health within the Data Linkage Unit.

ECSA remains responsible for the secure transfer of personal information in line with the IPPs.

This exemption is conditional on SA NT DataLink having a current Joint Venture Consortium Agreement in place.

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 21 February 2016 to 31 December 2020. An extension may be negotiated with the Privacy Committee if required.

Simon Froude
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
8 December 2015