Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2010

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

September 2010

For information and advice, please contact:

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

ph: (08) 8204 8786
fax: (08) 8204 8777
e-mail: privacy@sa.gov.au

This annual report has been issued pursuant to Clause 4A(1) of the Proclamation of the Privacy Committee of South Australia.

The Hon Paul Holloway MLC
MINISTER ASSISTING THE PREMIER IN PUBLIC SECTOR MANAGEMENT

Dear Minister

The Privacy Committee of South Australia is pleased to provide you with this report of its activities for the year ending 30 June 2010. The report is provided pursuant to Clause 4A(1) of the *Proclamation establishing the Privacy Committee of South Australia*, as amended and republished in the South Australian Government Gazette on 11 June 2009.

Terry Ryan
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

30 September 2010

Table of Contents

1 Introduction

This is a report of the activities of the Privacy Committee of South Australia (the Privacy Committee) for the year ending 30 June 2010. It has been developed pursuant to Clause 4A (1) of the Proclamation establishing the Privacy Committee (see Appendix B).

The work undertaken by the Privacy Committee in 2009-10 took place in the context of significant increase in the profile of privacy in South Australia and Australia more broadly. Notably, Commonwealth, State and Territory governments took further steps forward in the reform of privacy law in Australia. This progress was due, in part, to the significant investment and commitment to electronic health reform through the Council of Australian Governments (COAG). A robust national privacy framework was viewed by COAG as essential to national electronic health initiatives.

The year also saw an increased profile for privacy issues generally within government, media and the broader community. Greater attention was given to community privacy concerns, particularly in relation to social networking, cyber safety and corporate information privacy breaches.

During 2009-10, the Privacy Committee provided advice that supported privacy policy reforms both in South Australia and at a national level. This included participating in consultations with the Commonwealth Government on improving the consistency of privacy law in Australia. In June 2010, the Commonwealth Government referred Exposure Draft Australian Privacy Principles (APPs) to the Senate Finance and Public Administration Committee for public consultation. The Privacy Committee was participating in the development of a South Australian Government submission in response to the draft APPs at the close of the financial year. The development of the draft APPs is an important step in the progression towards national consistency in privacy law.

The Privacy Committee also contributed to consultation processes relating to the further development of national electronic health initiatives during the year. It is a challenge for governments across Australia to ensure the benefits of technological advances in health service delivery are realised while maintaining appropriate protections against harm to individual privacy. A major milestone for the reform of electronic health during 2009-10 was the establishment of the Individual Healthcare Identifier and the national Health Care Identifier Service (see item 3.2).

The Privacy Committee continued to support State Government agencies in the application of the Information Privacy Principles (IPPs) and the promotion of good privacy practice. This included responding to requests for advice, developing new privacy information sheets and conducting privacy awareness training.

During the reporting year, the Privacy Committee granted 15 exemptions from the IPPs to State Government agencies (see item 3.7), concluded 10 of 14 complaints (see item 3.6) and contributed to a number of consultation programs and inquiries (see items 3.2 and 3.3). The Executive Support to the Privacy Committee received a slight increase in total enquiries from the public and State Government agencies compared to the previous year (see item 2.2.4).

2 South Australian Public Sector Privacy Framework

2.1 The Information Privacy Principles

South Australia's Information Privacy Principles (IPPs) were introduced in July 1989 by means of *Cabinet Administrative Instruction 1/89*, issued as *Premier & Cabinet Circular No. 12*, and more commonly known as the Information Privacy Principles Instruction.

The IPPs regulate the way South Australian Public Sector agencies collect, use, store and disclose personal information. A link to the Information Privacy Principles Instruction can be found on the State Records website at www.archives.sa.gov.au/privacy, and in Appendix A of this report.

2.2 The Privacy Committee of South Australia

2.2.1 Establishment and Functions

The Privacy Committee was established by Proclamation in the Government Gazette on 6 July 1989. The functions of the Privacy Committee, as described in this Proclamation, are:

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

The scope of these functions is broader than the application of the IPPs and not necessarily restricted to activity within the South Australian Public Sector. However, the primary focus of the available resources (see item 2.2.4) is on matters that carry the greatest impact on the handling of personal information within State Government agencies bound by the IPPs.

A copy of the Proclamation can be found following the Information Privacy Principles Instruction, and in Appendix B of this report.

2.2.2 Reporting

During 2009-10, the Privacy Committee reported to the Hon Jay Weatherill MP, Minister Assisting the Premier in Cabinet Business and Public Sector Management and from 25 March 2010 to the Hon Paul Holloway MLC, Minister Assisting the Premier in Public Sector Management.

2.2.3 Membership

There are six members of the Privacy Committee:

- three nominated by the Minister responsible (one of whom is not a public sector employee and one of whom will have expertise in information and records management)
- one nominated by the Attorney-General
- one nominated by the Minister for Health
- one nominated by the Commissioner for Public Employment.

For this reporting year, the Privacy Committee comprised:

Presiding Member:

- Terry Ryan, Director, State Records of South Australia, Department of the Premier and Cabinet

Members, in alphabetical order:

- Samantha Doherty, non-public sector employee (commenced November 2007 and resigned August 2009)
- Tanya Hosch, non-public sector employee (commenced February 2010)
- Andrew Mills, Chief Information Officer, Government of South Australia (commenced November 2009)
- Bernadette Quirke, Legal Counsel, Projects Branch, Department of Treasury and Finance, Crown Solicitor's Office
- Christopher Radbone, Principal Consultant, Governance, Department for Environment and Heritage (commenced March 2008 and resigned September 2009)
- Nancy Rogers, Manager, Research, Media and Communication, Department for Families and Communities
- Andrew Stanley, Director, Policy, Legislation and Research, SA Health.

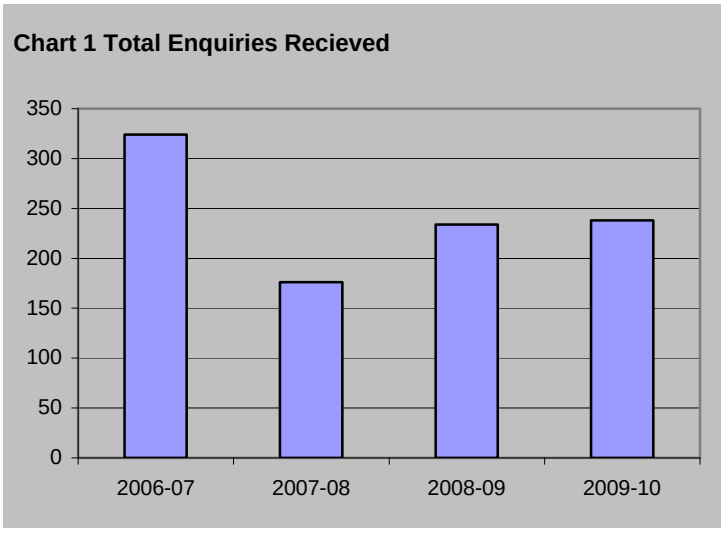
The term of appointment for each of the current members expires on 9 November 2010.

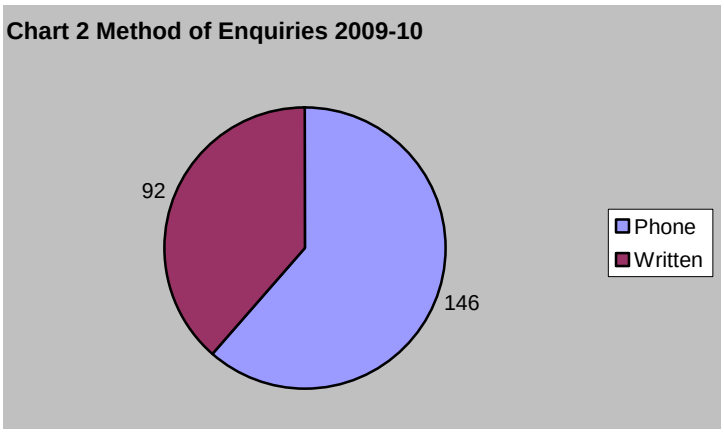
2.2.4 Resources

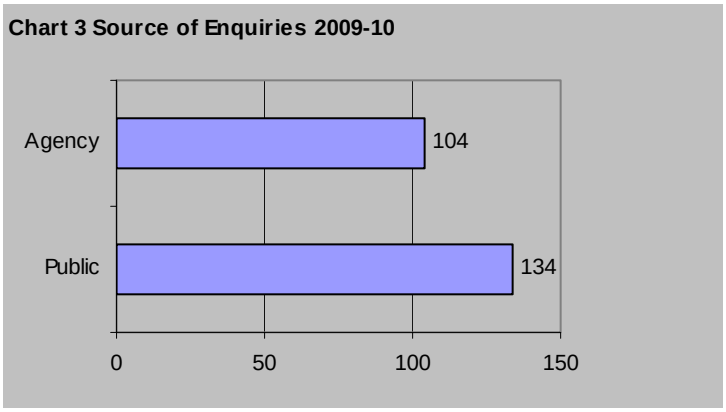
State Records of South Australia (State Records) provides support to the Privacy Committee including administrative support and meeting coordination, web hosting, an enquiry and advice service to both agencies and the public and a limited research function. This resource includes the commitment of approximately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

2.2.4.1 Privacy Enquiries

During the reporting year State Records responded to 238 telephone and email enquiries from the public and State Government agencies relating to privacy of personal information. While there was an increase in email and other written enquiries of 54 on the previous year there was a decrease in telephone enquiries of 50 on the previous year.







2.2.4.2 Privacy Training

Throughout the year, State Records conducted two Privacy Awareness training sessions for State Government employees. Privacy awareness is also included

in the curriculum for the nationally accredited Certificate III in Business (Recordkeeping), developed and delivered by State Records.

2.2.5 Committee Remuneration

Premier & Cabinet Circular No. 16: Remuneration for Government Appointed Part-time Boards and Committees specifies the conditions under which members of Boards and Committees may be remunerated. In general, fees are not paid to Government employees, and so only the non-government member of the Privacy Committee received a sessional fee for meetings attended. The sessional fees are drawn from State Records' recurrent operating budget. More information about the payment of fees can be found at *Premier & Cabinet Circular No. 16* available at www.premcab.sa.gov.au/pdf/circulars/Remuneration.pdf.

2.2.6 Meetings

During the reporting year the Privacy Committee met on six occasions. 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 contains a brief history of privacy law and self-regulation in South Australia, and an overview of the protection of personal information in other Australian jurisdictions. The handbook also contains a Code of Conduct for members consistent with *Government Boards and Committees: Guidelines for Agencies and Board Directors* (Department of Premier and Cabinet, 2000).

A copy of the handbook can be found on the State Records website at www.archives.sa.gov.au/privacy/committee.html.

2.2.8 South Australia's Strategic Plan

South Australia's Strategic Plan 2007 (Strategic Plan) calls for performance improvement across the South Australian Public Sector in both government decision-making and administrative efficiency (Objective 1: Growing Prosperity: Targets T1.8 and T1.9). The Privacy Committee continues to improve in this area by implementing strategies such as the conduct of business out of session where appropriate to do so. In addition, improvements were made to the Privacy Committee's processes to improve decision making and increase efficiency in the handling of complaints and enquiries from members of the public.

The constitution of the Privacy Committee meets Target T5.1 (Objective 5: Building Communities) to *'increase the number of women on all State Government boards and committees to 50% on average by 2008'*. During the reporting year the Privacy Committee maintained 50% female membership.

The activities of the Privacy Committee contribute to the achievement of other South Australia's Strategic Plan targets and priority actions across the South Australian Public Sector. Examples include:

- Objective 1: Growing Prosperity: Target T1.7: *'performance in the public sector – customer and client satisfaction with government services'* – the Australian public expects a high degree of privacy protection when accessing government services, and also expect a degree of control over how their personal information will be collected, stored, used and disclosed. There is also a high level of expectation and trust by the public that personal information held by State Government agencies is safe.
- Objective 2: Improving Wellbeing: there is a growing need for more holistic research and development in the areas of health, wellbeing and public safety. The use of personal information for research requires consideration of the IPPs to ensure the information is appropriately managed during and after completion of these activities.
- Objective 5: Building Communities: Priority Actions: *'collaborate to improve access to services and increase… resource sharing'*; and Objective 6: Expanding Opportunity: all targets – there has been a marked increase in data matching and information sharing activities. This presents a challenge for agencies in their obligations to comply with the IPPs when handling personal information.

3 Activities of the Privacy Committee

3.1 Advice to the Minister

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

Throughout the reporting year, the Privacy Committee briefed the Minister on a range of matters relating to privacy. This included briefings related to national consistency in privacy law in Australia, privacy and e-health reform initiatives and the development of privacy legislation for South Australia. The Privacy Committee also provided advice to the Minister in relation to State Government initiatives that had the potential to impact on the privacy of individuals in South Australia.

3.2 Developments in other jurisdictions

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

3.2.1 Commonwealth, States and Territories

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

3.2.1.1 Australian Privacy Law Reform

In October 2009, the Commonwealth Government released its first stage response to the Australian Law Reform Commission (ALRC) Report 108, *For Your Information Australian Privacy Law and Practice*. The response addressed 197 of the ALRC's 295 recommendations. 'The focus of the first stage response was to establish the foundations for an enhanced privacy framework'[1].

As outlined in its response the Commonwealth Government made a number of commitments, most notably, to:

- develop a single set of privacy principles in the Commonwealth Privacy Act, which will pave the way for pursuing national consistency of privacy law through discussion with State and Territory Governments;
- create a comprehensive credit reporting framework;
- improve health sector information flows; and
- strengthen the Privacy Commissioner's powers.

In line with its response, the Commonwealth Government began discussions with State and Territory Governments in February 2010 on the best method for progressing the achievement of national consistency in Australian privacy law.

The Privacy Committee contributed the South Australian Government's response to these consultations.

The work of the Commonwealth Government in response to the ALRC's Report 108 during 2009-10 culminated in the release of exposure draft Australian Privacy Principles (APPs) on 24 June 2010. The exposure draft APPs are seen as an important first step toward achieving national consistency in privacy law. The exposure draft APPs were immediately referred to the Senate Finance and Public Administration Committee for public consultation. At the close of the financial year, the Privacy Committee was involved in the development of the South Australian Government submission to the consultation.

Two key issues were identified from the perspective of the Privacy Committee:

- the failure of the Commonwealth to deal with the specific requirements in relation to health information within the exposure draft APPs. South Australia's position in responding to the ALRC Review had been that any specific health information requirements should be dealt with in the body of the APPs
- the absence of any provision within the exposure draft APPs for the collection, use and disclosure of information for the purposes of research in the public interest.

The draft APPs represent an improvement on the State's current IPPs supporting a better balance in privacy protection of information, and recognising the importance of developments in collaborative government, particularly in the areas of social inclusion, law enforcement and the prevention of crime.

3.2.1.3 National Electronic Health Reform

Electronic health reform continued to be a focus for governments across Australia during the year. Two key milestones in the reform were reached, including the:

- signing of the National Partnership Agreement on E-health Reform through the Council of Australian Governments (COAG)
- establishment of the Healthcare Identifiers Service (HI Service).

At the COAG meeting on 7 December 2009, the South Australian Government, along with other Commonwealth, State and Territory Governments, became a signatory to the *National Partnership Agreement on E-Health Reform* (Agreement).

This Agreement will contribute to an improved health system for all Australians through the development of a world class electronic health capability. It includes the establishment of the national Health Care Identifier Service (HI Service), which provides a national capability to uniquely identify each person or healthcare provider accessing or providing healthcare services within Australia. The HI Service underpins the development of a national electronic health system. Under the Agreement, Commonwealth, State and Territory Governments agreed to the coordination of regulators and the establishment of a uniform privacy framework to support e-health reform.

The Privacy Committee was involved in two consultations on the development and implementation of the HI Service during the year, which were:

- response to the Australian Health Ministers' Advisory Council *Discussion Paper on Healthcare and Identifiers and privacy* that related to the legislative proposals to support the introduction of Individual Healthcare Identifiers and health provisions of the proposed national privacy framework
- South Australian Government's Submission on the *Healthcare Identifiers Bill 2010.*

The Commonwealth *Healthcare Identifiers Act 2010* commenced on 29 June 2010 and the HI Service began on 1 July 2010.

3.2.1.4 Other Commonwealth and National initiatives

During the year, the Privacy Committee was involved in consultation on the privacy arrangements under the National Registration and Accreditation Scheme (the Scheme) for the health professions. The Scheme will regulate ten health professions under nationally consistent legislation and will be overseen by a Ministerial Council and an independent Australian Health Workforce Advisory Council. A national agency will administer the Scheme and support national profession-specific boards. The national agency will have a presence in each state and territory. The *Health Practitioner Regulation National Law (South Australia) Act 2010* (the National Law) came into effect on 1 July 2010.

The National Law will have its own provisions for regulating privacy under the Scheme. This will relate to the personal information handled by any of the bodies established by the Scheme. The privacy provisions are based on the Commonwealth *Privacy Act 1988* and modified by regulation under the National Law for application in the Scheme.

The Privacy Committee also provided advice to support the South Australian Government in its negotiations on the privacy arrangements for the development of proposed National Heavy Vehicle regulation.

3.2.2 Conferences and seminars

Throughout the year, representation of the Privacy Committee at various conferences, seminars and forums, included attendance at:

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

3.2.2.1 APPA

APPA convenes twice a year with meetings hosted on a rotating basis by the various Privacy Commissioners. At the meetings, issues are discussed such as privacy and security, identity management, surveillance, cross-jurisdictional law enforcement between countries in the Pacific Rim, privacy legislation amendments, cryptography and personal data privacy. The Privacy Committee has observer status at APPA as it is not considered an independent statutory body.

On 3 and 4 December 2009, the Privacy Committee hosted the 32nd meeting of APPA in Adelaide. The meeting was attended by representatives of Privacy

Authorities from the United States (Office of the Federal Trade Commissioner), Korea, New Zealand, and Australian jurisdictions including the Australian Privacy Commissioner, Victoria, New South Wales, Queensland, Northern Territory and the Australian Capital Territory. The New Zealand Privacy Commissioner and the Hong Kong Privacy Commissioner for Personal Data participated in the meeting by teleconference.

A representative of the Privacy Committee also attended the 33rd meeting of APPA in Darwin on 3 and 4 June 2010.

The issues addressed at the APPA meetings for 2009-10 included:

- general privacy issues in jurisdictions, including future privacy impacts of cloud computing and the use of biometric data for entry into nightclub venues;
- establishment of a Technology Working Group within APPA;
- progress towards Global Privacy Enforcement Network and Global Privacy Standard;
- APEC Privacy Framework and outcomes from the 31st International Conference of Data Protection and Privacy Commissioners; and
- establishment of a working party to review of APPA's membership criteria.

Further information about APPA can be found on the Commonwealth Privacy Commissioner's website at
http://www.privacy.gov.au/international/appa/index.html

At the 33rd meeting of APPA members resolved to find a mechanism by which authorities that perform functions substantially similar to APPA members would be eligible to join.

3.2.2.2 Privacy and Identity Security forum

On 4 December 2009, the Privacy Committee hosted a forum on *Privacy, Identity and E-Crime* in conjunction with the APPA meeting held in Adelaide.

The forum featured presentations on:

- electronic and identity crime prevention;
- balancing privacy and security in the e-passport system;
- information and identity security in government; and
- youth privacy and electronic crime issues.

Presenters at the forum included the Australian and Victorian Privacy Commissioners, the Commercial and Electronic Crime Branch of South Australia Police, the Office of the Chief Information Officer and a PhD Candidate from the University of South Australia.

Over 150 representatives of State and Commonwealth government agencies, Non-government organisations and the general public attended the forum.

3.2.2.3 Privacy Authorities of Australia (PAA)

The Privacy Committee was represented at the meeting of the PAA on 17 September 2009.

PAA is a group of privacy authorities from Australian jurisdictions that meet informally to encourage knowledge sharing and cooperation on privacy issues specific to Australia.

The PAA terms of reference include:

- facilitating the sharing of knowledge and resources between privacy agencies and authorities within Australia;
- fostering cooperation in privacy and data protection;
- promoting best practice and consistency amongst privacy agencies and authorities; and
- working to continuously improve our performance to achieve the important objectives set out in our respective privacy laws or policies.

The PAA meeting on 17 September 2009 addressed a number of issues across Australian jurisdictions, including:

- model spent convictions legislation;
- development of an emergency telephone warning system;
- use of automated number plate recognition technology; and
- surveillance in public places and social networking.

3.3 Recommendations and submissions

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

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

3.3.1 Implementation of Amendments to the Information Privacy Principles (IPPs)

On 18 May 2009, Cabinet approved amendments to the IPPs to recognise the activity of businesses performing services on behalf of government. These amendments addressed the gap that existed in the application of privacy principles to service providers contracted to the South Australian Government.

The work undertaken to progress the implementation of the amendments during the year included:

- developing an information sheet on Contracting and the IPPs;
- developing a short guide to the IPPs;
- finalising the model terms and conditions in consultation with the Crown Solicitor's Office; and
- extending the exemption from IPP 10 to allow agencies twelve months to include model privacy terms and conditions into contracts.

The amendments to the IPPs complement the Contracting and Official Records Standard (the Standard) issued under the *State Records Act 1997*. The Standard was developed by State Records to ensure that records collected or created by service providers under contract to South Australian Government agencies are managed in line with the State Records Act.

3.3.2 SA NT DataLink

SA NT DataLink is the operational body of a joint venture consortium of South Australian and Northern Territory Government agencies and non-government organisations and universities. SA NT DataLink is responsible for the development, maintenance and operation of a Data Linkage System (the System) that allows research projects to be undertaken with de-identified data in South Australia and the Northern Territory. The System is aimed at providing an improved evidence base for research, while minimising risks to individual privacy when compared to traditional sample based research methods.

SA NT DataLink was officially launched on 12 November 2009. The first two research projects to use the System were progressed during the year, namely:

- early childhood development demonstration project; and
- colorectal cancer demonstration project.

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

During 2009-10, the Privacy Committee continued to work with SA NT DataLink on the privacy and governance arrangements for the System and provided advice on its development. In addition, the Privacy Committee provided three exemptions from the IPPs to facilitate the further establishment of the System. These exemptions were provided where the Privacy Committee deemed them to be in the public interest.

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

3.3.4 Family Safety Framework

During the year, the Privacy Committee was consulted on the expansion of the Family Safety Framework (Framework) established by the Office for Women. The Framework was established to improve and integrate service responses to violence against women and children in South Australia. Specifically, the Framework provides for cases of domestic/family violence assessed as high risk to be referred to a local family safety meeting. The meeting is attended by a range of agencies that provide service responses to victims of domestic violence.

The Privacy Committee endorsed the expansion of the Framework and provided advice on the development of agreements between agencies attending the family safety meetings to promote the protection of personal information.

3.3.5 Data Matching by Courts Administration Authority

The Privacy Committee was consulted on the expansion of the data matching program undertaken by the Fines Payment Unit (FPU) in the Courts Administration Authority (CAA). The data-matching program enables the FPU to fulfill its legislative obligations to locate fine debtors for the collection of fines by matching data FPU data with data from the South Australia Police. The FPU sought to extend the program to also match data with SA Water.

As recommended by the Privacy Committee, the FPU undertook a Privacy Impact Assessment (PIA) of the data-matching program to identify any privacy risks and demonstrate that the program would comply with the Information Privacy Principles. The FPU advised the public of the extension of the data matching program by notification in *The Advertiser*, *Government Gazette* and the CAA website.

3.3.6 State Recovery Operations Manual

Towards the end of the reporting year, the Privacy Committee began work with the State Recovery Office (SRO) on reviewing the privacy arrangements for the State Recovery Operations Manual. The Operations Manual is a guide for those undertaking a recovery coordination role after a State emergency. The Privacy Committee provided interim advice for inclusion in the manual and agreed to work further with the SRO to ensure the appropriate sharing and management of personal information during emergency recovery operations.

3.4 Communication

The Privacy Committee has the function, under clause 2(c) of the Proclamation, *'to make publicly available, information as to methods of protecting individual privacy and measures that can be taken to improve existing protection'*.

3.4.1 Privacy Officer Network

The Privacy Officer Network (the Network) was established in September 2006 to assist Principal Officers of agencies fulfill their obligation to comply with the IPPs, and to increase the efficiency of communications about the handling of personal information held by State Government agencies. State Records coordinates and provides support to the Network. The aim of the Network is to contribute to the improvement of privacy awareness across the public sector.

No formal meetings of the Privacy Officer Network were held during 2009-10, however members of the Network were personally invited to attend the Privacy Committee's public Privacy and Identity Security Forum held in December 2009. The Network was also advised of significant developments in privacy throughout the 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.

The Privacy Committee is represented on the South Australian Identity Security and Management Group, APPA (see also item 3.2.3.1) and PAA (see also item 3.2.3.2).

The Presiding Member is also a member of the South Australian Government's ICT Security and Risk Steering Committee.

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. See section 3.3.

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'*.

During the reporting year there were 13 new formal complaints received and one pre-existing complaint that underwent further deliberation. Of the 14 complaints handled, 10 were concluded and four remained outstanding. A summary of the complaints concluded during the year is outlined in the table below.

3.6.1 Complaint Summary Table

	Respondent Organisation	**Information Privacy Principle (IPP)**	**Other Privacy Issue**	**Outcome**
1	Statutory Authority	IPP 2, 8&10		Agency apology, amendment of agency practices
2	Government Department	IPP 10		No breach of the IPPs determined
3	Government Department	IPP 8 &10		No breach of the IPPs determined
4	Government Department	IPP 8&10		Privacy Committee unable to handle – concerned employee of the Crown
5	Law Enforcement	IPP 8&10		Referred to Police Complaints Authority
6	Local Government		Disclosure	Privacy Committee wrote to Council recommending review of practice
7	Private Organisation		Surveillance	Privacy Committee provided advice on relevant authority to deal with complaint
8	Government Department	IPP 10		No breach of the IPPs determined
9	Statutory Authority	IPP 10		Complaint lacking substance
10	Law Enforcement	IPP 10		Referred to Police Complaints Authority

The Privacy Committee took a number of steps during the year to improve the management and visibility of its complaints handling function. This included significant changes to the information available through the State Records website, improving its presence on the www.sa.gov.au website and considering options for processing complaints more efficiently.

3.6.2 Complaint Case Studies

Example 1 - IPP 8 and 10

A complainant alleged that a Statutory Authority disclosed their personal home address to a third party. The complainant alleged that the home address was collected by the Authority in relation to an unrelated matter but subsequently disclosed to the third party.

The Privacy Committee wrote to the Authority seeking a response to the complaint. In its response to the Privacy Committee, the Statutory Authority admitted that the disclosure of the personal information was an error made by one of its support staff that mistakenly believed that there was a lawful requirement for the information to be disclosed. The Statutory Authority apologised to the complainant for the disclosure and noted on its records management system that the complainants' home addresses were to remain confidential. It also advised its staff not to place the complainant's address on any document that might come to the attention of a third party.

Example two – IPP 8 and 10

A complainant alleged that an officer of a Government agency had accessed her personal address information from the agency's records and used the information to send her a threatening letter. The complainant indicated that her address information was not publicly available. The complainant had raised her concerns with the agency but was dissatisfied with the initial response.

The Privacy Committee referred the complaint back to the agency concerned for a response. The agency's response outlined that they had investigated the complaint and found no evidence to suggest the officer had accessed the agency's records to obtain the complainant's address. It also indicated that the officer did not have general access to the electronic database where the records were held. The agency indicated that the officer had also denied accessing records to obtain the information. The Privacy Committee considered the agency's response and was satisfied that an infringement of the Information Privacy Principles had not occurred.

3.6.2 Local Government complaints

The Privacy Committee received two formal privacy complaints concerning Local Government Authorities during 2009-10. One of the complaints concerned a Council's compliance with its own privacy policy and the other concerned video surveillance by a Council. In regard to the first complaint, the Privacy Committee wrote to the Council and recommended it ensure its practices aligned with its privacy policy. The second complaint was referred to the Local Government Association.

These complaints highlight the ongoing difficulties that apply in relation to the management of personal information in Local Government Authorities in South Australia. The Privacy Committee has limited functions to deal with such complaints and in some cases there may be no other formal avenue independent of the Council to resolve the matter. There is currently no legislative or administrative privacy regime applying to Local Government in South Australia.

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 public interest for an activity outweighs the privacy protections afforded by the IPPs, or where otherwise warranted by unique circumstances. Exemptions are generally subject to conditions including an expiry date and agencies reporting on the activity conducted under the exemption.

During this reporting year, 15 individual exemptions were approved. Following is a summary of each of the requests for exemption.

3.7.1 BASS – Patron Ticketing Information

In December 2008, the Privacy Committee granted an exemption to the Adelaide Festival Centre Trust in relation to the BASS Ticketing agency to permit disclosure of patron ticketing information to Flagship Arts Companies, such as Adelaide Symphony Orchestra and State Theatre Company.

The Flagship Arts Companies sought the information to enable them to contact their patrons direct to provide them with further information about upcoming shows, pre-show events and activities. The exemption was to allow BASS to upgrade its ticketing system to collect patron consent to the disclosure.

The procurement of a new ticketing system for BASS was delayed requiring BASS to seek two extensions to the original exemption during 2009-10. The Privacy Committee granted the exemptions on the condition that Flagship Arts Companies offered patrons the opportunity to opt-out of any further correspondence each time they are contacted and that patron information is otherwise managed in line with the IPPs.

See Appendix C for the full text of the exemptions.

3.7.2 Contracted Service Providers

On 18 May 2009, Cabinet approved amendments to the IPPs to recognise the activity of businesses performing services on behalf of government. These amendments addressed the gap that existed in the application of the IPPs to service providers contracted to the South Australian Government. As part of the amendments, model privacy clauses were developed for government contracts that addressed the handling of personal information. State Records undertook substantial consultation on the changes with all stakeholders within Government.

To facilitate transition towards full compliance with the amended IPPs, in June 2010 the Privacy Committee granted an exemption from IPP 10 to all agencies to allow disclosure of personal information to contracted services providers under existing contracts. The exemption was conditional on agencies progressively including privacy terms and conditions in all contracts that involve the handling of personal information.

See Appendix D for the full text of the exemption.

3.7.3 Early Intervention Pilot Project

In February 2010, the Privacy Committee received a request for exemption from IPPs 2 and 8 from the Office of Crime Statistics and Research (OCSAR) in relation to the Early Intervention Pilot Project (Pilot Project) being undertaken by South Australia Police and Drug and Alcohol Services SA (DASSA).

The aim of the Pilot Project is to provide an option for South Australian Police officers to divert young people apprehended for alcohol related offences to a health intervention program rather than process them through the criminal justice system.

The Privacy Committee received a further request for exemption from IPPs 2 and 10 from South Australia Police and DASSA for the operational aspects of the Pilot Project and the Police Drug Diversion Initiative (PDDI). The PDDI provides a diversion option similar to the Pilot Project for adults and young people apprehended for simple possession drug offences.

The Privacy Committee granted the exemptions on 14 April 2010. The exemption in relation to the evaluation of the Pilot Program by OCSAR was conditional on approval for the evaluation being granted by the South Australian Health Human Research Ethics Committee.

See Appendix E for the full text of the exemptions.

3.7.4 Offender Management Plan

In February 2010, the Privacy Committee received a joint submission from South Australia Police, the Department for Correctional Services, the Department for Families and Communities and the Department of Health for an exemption from IPPs 2, 8 and 10 to allow for information sharing between the agencies through a pilot program of the South Australia Offender Management Plan (the Plan). The purpose of the Plan is to provide coordinated case management of serious adult offenders who present the most harm to the community in order to improve rehabilitation outcomes and promote community safety.

The exemption was restricted to information relevant to the coordinated case management of the selected offenders under the pilot program and conditional on those offenders being informed of their inclusion in the pilot program.

See Appendix F for the full text of the exemption.

3.7.5 DTEI Way2Go

In November 2009, the Privacy Committee received a submission from the Department for Transport Energy and Infrastructure (DTEI) seeking a review and extension of a current exemption from IPPs 8 and 10 in relation to the Way2Go Program.

The exemption allowed DTEI to use public school student address information collected from the Department of Education and Children's Services (DECS) for a Geospatial Information Systems (GIS) mapping project that would focus on promoting safer and more active student travel to public schools. A primary outcome of the mapping project would be the development of school route maps that indicated safe and efficient routes to school and assisted with planning active travel and transport engineering and infrastructure development around schools.

The exemption included strict conditions on access to personal information and any GIS maps that indicated the specific location of student home addresses. It also recommended that a memorandum of understanding be established between the two agencies that outlined the information sharing arrangement.

The Privacy Committee agreed to extend the exemption for three years. The exemption was also modified to allow DTEI's Community Education and Programs staff to provide supervised access to the GIS maps to selected 'focus teachers' from relevant South Australian public schools for the purposes of developing school travel plans.

See Appendix G for the full text of the exemption

3.7.6 SA NT DataLink

The Privacy Committee received two submissions from the SA NT DataLink Consortium during the year seeking exemptions from the IPPs. The exemptions were sought in line with the governance arrangements established between the Privacy Committee and SA NT DataLink to facilitate the development of the Data Linkage System.

In October 2009, the Privacy Committee received a submission from SA NT DataLink seeking exemptions permitting the use of the Families SA data set and the Public Schools Enrolment data set in the establishment of the Master Linkage File of the Data Linkage System.

The Privacy Committee granted an exemption to the Department of Families and Communities to disclose limited identifying variables from the Families SA dataset to SA NT DataLink. It also granted an exemption to the Department of Education and Children's Services to disclose limited identifying variables from the public school enrolment data set to SA NT DataLink. The Privacy Committee granted exemptions to the Department of Health to use the limited variables from the data sets in the establishment of the Data Linkage System. The exemptions were conditional on the Department of Health ensuring that the information was only accessible by officers of the Department within SA NT DataLink.

See 3.3.2 for more information on the SA Data Linkage Project and Appendix H for the full text of the exemptions

Endnotes:

[1] Australian Government, *Enhancing National Privacy Protection Australian Government First Stage Response to the Australian Law Reform Commission Report 108*, October 2009, p.9

Appendices

A Information Privacy Principles

Cabinet Administrative Instruction 1/89, also known as the Information Privacy Principles (IPPs) Instruction, and premier and cabinet circular 12, AS AMENDED BY CABINET 18 May 2009

Government of South Australia

Cabinet Administrative Instruction No.1 of 1989

(Re-issued 30 July 1992 and 18 May 2009)

PART 1
PRELIMINARY

Short Title

1. This Instruction may be called the "Information Privacy Principles Instruction".

Commencement and Application

2. (1) This Instruction will come into effect on 18 May 2009.

(2) Subject to any contrary determination by Cabinet, this Instruction shall apply to "the public sector agencies" as that expression is defined in Section 3(1) of the *Public Sector Management Act 1995.*

(3) This Instruction shall not apply to an agency that appears in the attached schedule.

Interpretation

3. (1) In this Instruction-

"agency" means a public sector agency that falls within the scope of application of this Instruction pursuant to the provisions of Clause 2(2).

"the Committee" means the Privacy Committee of South Australia constituted by Proclamation.

“contracted service provider” means a third party that enters into a contract with an agency to provide goods or services required by an agency for its operations.

“contract for service” means that contract between the contracted service provider and the agency.

"personal information" means information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person

whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

"principal officer" means in relation to an agency:

(a) the person holding, or performing duties of, the Office of Chief Executive Officer of the agency;

(b) if the Commissioner for Public Employment declares an office to be the principal office in respect of the agency - the person holding, or performing the duties of, that office; or

(c) in any other case - the person who constitutes that agency or, if the agency is constituted by two or more persons, the person who is entitled to preside at any meeting of the agency at which the person is present.

"the Principles" means the Information Privacy Principles established under Clause 4 of this Instruction.

"record-subject" means a person to whom personal information relates.

(2) A reference to any legislation, regulation or statutory instrument in this Instruction shall be deemed to include any amendment, repeal or substitution thereof.

(3) A reference to a person, including a body corporate, in this Instruction shall be deemed to include that person's successors.

PART II
INFORMATION PRIVACY PRINCIPLES

Principles

4. The principal officer of each agency shall ensure that the following Principles are implemented, maintained and observed for and in respect of all personal information for which his or her agency is responsible.

Collection of Personal Information

(1) Personal information should be not collected by unlawful or unfair means, nor should it be collected unnecessarily.

(2) An agency that collects personal information should take reasonable steps to ensure that, before it collects it or, if that is not practicable, as soon as practicable after it collects it, the record-subject is told:

(a) the purpose for which the information is being collected (the "purpose of collection"), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law - that the collection of the information is so authorised or required; and

(c) in general terms, of its usual practices with respect to disclosure of personal information of the kind collected.

(3) An agency should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out of date, incomplete or excessively personal.

Storage of Personal Information

(4) An agency should take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused.

Access to Records of Personal Information

(5) Where an agency has in its possession or under its control records of personal information, the record-subject should be entitled to have access to those records in accordance with the *Freedom of Information Act 1991*.

Correction of Personal Information

(6) An agency that has in its possession or under its control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, incomplete, irrelevant, out of date, or where it would give a misleading impression in accordance with the *Freedom of Information Act 1991*.

Use of Personal Information

(7) Personal information should not be used except for a purpose to which it is relevant.

(8) Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless:

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

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

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

(d) the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

(9) An agency that uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of Personal Information

(10) An agency should not disclose personal information about some other person to a third person unless:

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

(b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person;

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

(d) the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

Acts and Practices of Agency and Contracted Service Provider

5. For the purposes of this Instruction-

(a) an act done or practice engaged in by, or personal information disclosed to, a person employed by, or in the service of, an agency in the performance of the duties of the person's employment shall be deemed to have been done or engaged in by, or disclosed to, the agency;

(b) an act done or practice engaged in by, or personal information disclosed to, a person on behalf of, or for the purposes of the activities of, an unincorporated body, being a board, council, committee, subcommittee or other body established by, or in accordance with, an enactment for the purpose of assisting, or performing functions in connection with, an agency, shall be deemed to have been done or engaged in by, or disclosed to, the agency.

(c) subject to clause 5(A), an act done or a practice engaged in by, or personal information disclosed to, a person employed by, or in the service of, a person or organisation providing services to an agency under a contract for services for the purpose of or in the course of performance of that contract shall be deemed to have been done or engaged in by, or disclosed to, the agency.

5(A) A contract for service, which will necessitate the disclosure of personal information to a contracted service provider, must include conditions to ensure that these Principles are complied with as if the Contracted Service Provider were part of the agency and must include provisions that enable audit and verification of compliance with these obligations.

Agencies to comply with Principles

6. An agency shall not do an act or engage in a practice that is in breach of or is a contravention of the Principles.

Collecting of Personal Information

7. For the purposes of the Principles, personal information shall be taken to be collected by an agency from a person if the person provides that information to the agency in response to a request by the agency for that information or for a kind of information in which that information is included.

PART III
COMPLIANCE WITH PRINCIPLES

8. The Committee may at any time on its own initiative appoint a person (whether or not that person is a public employee) or the Commissioner for Public Employment to investigate or assist in the investigation of the nature and extent of compliance of an agency with the Principles and to furnish a report to the Committee accordingly.

Reporting Procedures Pursuant to this Instruction

9. Each principal officer shall furnish to the Committee such information as the Committee requires and shall comply with any requirements determined by the Committee concerning the furnishings of that information including:

   (a) the action taken to ensure that the Principles are implemented, maintained and observed in the agency for which he or she is responsible;

   (b) the name and designation of each officer with authority to ensure that the Principles are so implemented, maintained and observed;

   (c) the result of any investigation and report, under Clause 8, in relation to the agency for which he or she is responsible and, where applicable, any remedial action taken or proposed to be taken in consequence.

Agencies Acting Singly or in Combination

10. This Instruction and the Principles shall apply to the collection, storage, access to records, correction, use and disclosure in respect of personal information whether that personal information is contained in a record in the sole possession or under the sole control of an agency or is contained in a record in the joint or under the joint control of any number of agencies.

SCHEDULE: CLAUSE 2 (3)
AGENCIES TO WHICH THIS INSTRUCTION DOES NOT APPLY

South Australian Asset Management Corporation

Motor Accident Commission (formerly State Government Insurance Commission)

WorkCover Corporation of South Australia

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.

C Exemption Granted – BASS Patron Ticketing Information

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee 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 Adelaide Festival Centre Trust (AFCT). It is an exemption from compliance with Principle 10, allowing BASS, a business unit within AFCT, to disclose personal information to the Flagship Arts Companies. The Flagship Arts Companies are:

- Adelaide Symphony Orchestra
- Adelaide Festival Centre Presents
- Australian Ballet
- Brink Productions
- State Opera of South Australia
- State Theatre Company
- Windmill Performing Arts.

The personal information to be disclosed is limited to the title, name, address, phone number(s), ticketing transaction history (specific to company receiving data) and email address of patrons of the Flagship Arts Companies.

The purpose of disclosure is to allow the Flagship Arts Companies to directly contact patrons who have purchased tickets to their performances.

All other Principles continue to apply.

Conditions

This exemption is conditional on BASS only disclosing patron information to a Flagship Arts Company that was collected in relation to a performance of that particular company. The exemption is also conditional on the Flagships Arts Companies providing patrons the option to opt-out of any further correspondence each time they contact patrons.

Prior to disclosing personal information under this exemption, BASS is to ensure that the Flagship Arts Companies receiving the information are subject to the Commonwealth *Privacy Act 1988,* or have an established privacy policy, that will contribute to the ongoing protection of the information provided by BASS.

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.

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

Expiry

This is an exemption for the transfer of the ticketing information to the Flagship Arts Companies for the period up to 31 August 2010.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

21 October 2009

Exemption

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

This exemption applies to the Adelaide Festival Centre Trust (AFCT). It is an exemption from compliance with Principle 10, allowing BASS, a business unit within AFCT, to disclose personal information to the Flagship Arts Companies. The Flagship Arts Companies are:

- Adelaide Symphony Orchestra
- Adelaide Festival Centre Presents
- Australian Ballet
- Brink Productions
- State Opera of South Australia
- State Theatre Company
- Windmill Performing Arts.

The personal information to be disclosed is limited to the title, name, address, phone number(s), ticketing transaction history (specific to company receiving data) and email address of patrons of the Flagship Arts Companies.

The purpose of disclosure is to allow the Flagship Arts Companies to directly contact patrons who have purchased tickets to their performances.

All other Principles continue to apply.

Conditions

This exemption is conditional on BASS only disclosing patron information to a Flagship Arts Company that was collected in relation to a performance of that particular company. The exemption is also conditional on the Flagships Arts Companies providing patrons the option to opt-out of any further correspondence each time they contact patrons.

Prior to disclosing personal information under this exemption, BASS is to ensure that the Flagship Arts Companies, receiving the information, are subject to the Commonwealth *Privacy Act 1988,* or have an established privacy policy that will contribute to the ongoing protection of the information provided by BASS.

---

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

Destruction or retention of personal information

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

Expiry

This is an exemption for the transfer of the ticketing information to the Flagship Arts Companies for the period up to 28 February 2011.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

25 May 2010

D Exemption Granted – Contracted Service Providers

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[3] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

The purpose of the exemption is to facilitate transition towards compliance with the amended Information Privacy Principles Instruction to allow disclosure of relevant personal information to contracted service providers under existing contracts.

This exemption applies to all agencies that fall within the scope of the Information Privacy Principles Instruction.

All other Principles continue to apply.

Conditions

1. Disclosure is allowed if it is required to satisfy an existing contract between an agency and a contracted service provider to provide goods or services required by the agency for its operations.
2. During the exemption period, the agency must make reasonable attempts to negotiate an in-principle agreement with the contracted service provider to adopt appropriate privacy practices where it is not possible or practical to include the terms and conditions in the contract.
3. During the exemption period, the agency must progressively include appropriate privacy terms and conditions in all contracts according to the following priorities:
    - contracts that handle more sensitive personal information (eg health records, religious or political views, detailed financial records)
    - contracts that do not already contain comparable privacy or confidentiality terms and conditions, or where the agency does not have a legislative mandate to disclose personal information to the contracted service provider.
    - in order to assess priority contracts, the agency must identify the risk to the personal information and to the continuation of the provision of goods or services.

Exclusions

This exemption applies only to those contracts that involve the handling of personal information.

This exemption does not apply to new contracts or contracts that come up for review or renewal.

---

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

Code of Fair Information Practice

The *Code of Fair Information Practice* (the Code) applies to the handling of personal information by the Department of Health and the Department for Families and Communities. Compliance with the Code already satisfies the provisions of the amended Information Privacy Principles Instruction and this exemption is therefore not applicable to these Departments. However these Departments may choose to rely upon this exemption should some gap in compliance be identified.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with the *State Records Act 1997* as described in the *Contracting and Official Records Standard*.

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).

Expiry

This exemption is provided for one year following its approval on 5 May 2010. If an agency believes that a contract cannot be renegotiated to include appropriate privacy terms and conditions within the exemption period, the views and assistance of the Privacy Committee of South Australia must be sought. The Privacy Committee will consider requests for additional exemptions on a case-by-case basis.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

23 June 2010

E Exemption Granted – Early Intervention Pilot Project

Exemption

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

This exemption applies to the Department of Health and specifically Drug and Alcohol Services South Australia. It is an exemption from compliance with Principles 2 and 10, allowing DASSA to collect personal information from the South Australia Police in relation to young persons suspected of alcohol related offences.

The personal information to be collected includes:

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)
- Date of birth (age)
- Gender
- Telephone contact details.

The purpose of collection and disclosure is to allow for the diversion of suspected young offenders to a health intervention through the Early Intervention Pilot Program and to facilitate the evaluation of that program by the Office of Crime Statistics and Research.

All other Principles continue to apply.

Conditions

This exemption is conditional on the provision of information on the nature of the referral and the diversion program to young persons diverted and their parents or guardians.

Security of Personal Information

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

Destruction or retention of personal information

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

---

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

Expiry

This exemption is provided for four years following its approval. DASSA is to report to the committee on the operation of the Pilot Program two years after the approval of this exemption. The report should highlight any privacy issues raised or complaints received in the operation of the Pilot Program. An extension to this exemption may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 April 2010

Exemption

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

This exemption applies to the Department of Health and specifically Drug and Alcohol Services South Australia (DASSA). It is an exemption from compliance with Principles 2 and 10, allowing DASSA to collect personal information from young persons suspected of simple possession drug offences from the South Australia Police.

The personal information to be collected and disclosed includes:

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)
- Date of birth (age)
- Gender
- Telephone contact details.

The purpose of collection and disclosure is to allow for the diversion of suspected young offenders to a health intervention through the Police Drug Diversion Initiative (PDDI) and to facilitate the evaluation of the PDDI by the Office of Crime Statistics and Research.

All other Principles continue to apply.

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

Conditions

This exemption is conditional on the provision of information on the nature of the referral and the diversion program to young persons diverted and their parents or guardians.

Security of Personal Information

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

Destruction or retention of personal information

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

Expiry

This exemption is provided for four years following its approval. DASSA is to report to the committee on the operation of the PDDI two years after the approval of this exemption. The report should highlight any privacy issues raised or complaints received in the operation of the PDDI. An extension to this exemption may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 April 2010

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[6] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the South Australia Police (SAPOL). It is an exemption from compliance with Principles 2 and 10, allowing SAPOL to collect personal information from young persons suspected of alcohol related offences and disclose them to the Drug and Alcohol Services South Australia's Drug Diversion Line.

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

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)

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

- Date of birth (age)
- Gender
- Telephone contact details.

The purpose of collection and disclosure is to allow for the diversion of suspected young offenders to a health intervention through the Early Intervention Pilot Program.

All other Principles continue to apply.

Conditions

This exemption is conditional on the provision of information on the nature of the referral and the diversion program to young persons diverted and their parents or guardians.

Security of Personal Information

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

Destruction or retention of personal information

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

Expiry

This exemption is provided for four years following its approval. SAPOL is to report to the committee on the operation of the Pilot Program two years after the approval of this exemption. The report should highlight any privacy issues raised or complaints received in the operation of the Pilot Program. An extension to this exemption may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 April 2010

Exemption

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

This exemption applies to the South Australia Police (SAPOL). It is an exemption from compliance with Principles 2 and 10, allowing SAPOL to collect personal information from young persons suspected of simple possession drug offences and to disclose that information to Drug and Alcohol Services South Australia's Drug Diversion Line.

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

The personal information to be collected and disclosed includes:

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)
- Date of birth (age)
- Gender
- Telephone contact details.

The purpose of collection and disclosure is to allow for the diversion of suspected young offenders to a health intervention through the Police Drug Diversion Initiative (PDDI).

All other Principles continue to apply.

Conditions

This exemption is conditional on the provision of information on the nature of the referral and the diversion program to young persons diverted and their parents or guardians.

Security of Personal Information

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

Destruction or retention of personal information

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

Expiry

This exemption is provided for four years following its approval. SAPOL is to report to the committee on the operation of the PDDI two years after the approval of this exemption. The report should highlight any privacy issues raised or complaints received in the operation of the PDDI. An extension to this exemption may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 April 2010

Exemption

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

or more of the Information Privacy Principles[8] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Attorney General's Department and specifically the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing OCSAR to collect and use personal information from the Drug and Alcohol Services South Australia's (DASSA's) Drug Diversion Line and offence data from the Justice Information System.

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

- Family name
- Given name
- Occupation
- Address
- Ethnicity (including language spoken and need for an interpreter)
- Date of birth (age)
- Gender
- Telephone contact details
- Information held on the Justice Information System (JIS) about record-cases' contact with the criminal justice system.

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

All other Principles continue to apply.

Conditions

This exemption is conditional on OCSAR obtaining approval for the evaluation from the South Australian Health Human Research Ethics Committee.

Security of Personal Information

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

Destruction or retention of personal information

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

Expiry

This exemption is provided for four years following its approval. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 April 2010

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

F Exemption Granted – Offender Management Plan

Exemption

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

This exemption applies to the South Australian Police (SAPOL), the Department for Correctional Services (DCS), the Department for Families and Communities (DFC) and the Department of Health (DH). It is an exemption from compliance with IPPs 2, 8 and 10, allowing SAPOL, DCS, DFC and DH, to share case file information of serious offenders as part of the Offender Management Plan Pilot Program (Pilot Program).

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

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

All other Principles continue to apply.

Conditions

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

The exemption is restricted to information relevant to the coordinated case management of selected serious offenders.

Security of Personal Information

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

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*.

---

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

Expiry

This exemption will expire one (1) year after its approval or at the end of the Pilot Program, which ever is earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 March 2010

G Exemption Granted – DTEI Way2Go

Exemption

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

This exemption applies to the Department for Transport, Energy and Infrastructure (DTEI). It is an exemption from compliance with IPPs 1,2,3,7 and 9, allowing DTEI, to collect personal enrolment information from the Department of Education and Children's Services (DECS) and use that information in the administration of the Way2Go program.

The personal information to be collected is: school name, enrolment, street name and number, for each student from participating schools. The information collected will not include the names of students.

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

All other Principles continue to apply.

Conditions

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

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

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

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

---

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

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

Destruction or retention of personal information

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

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

Expiry

DTEI and the Privacy Committee will review this exemption three (3) years after its approval. An extension may be negotiated with the Privacy Committee if required. DTEI is required to report to the Privacy Committee on the progress of the Way2Go program twelve (12) months after the approval of this exemption.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

24 December 2009

Exemption

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

This exemption applies to the Department of Education and Children's Services (DECS). It is an exemption from compliance with IPP 10, allowing DECS to disclose personal enrolment information to the Department for Transport, Energy and Infrastructure (DTEI) to the Way2Go Program.

The personal information to be disclosed is limited to: school name, enrolment, street name and number, for each student from participating schools. The information disclosed will not include the names of students.

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

All other Principles continue to apply.

Conditions

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

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

Destruction or retention of personal information

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

As duplicates of the official records held by DECS, the records collected by DTEI from DECS are to be destroyed following the creation of the associated GIS maps, in accordance with Normal Administrative Practice as described in Government Disposal Schedule 15, issued under the *State Records Act 1997*.

Expiry

DTEI and the Privacy Committee will review this exemption three (3) years after its approval. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

24 December 2009

H Exemption Granted – SA NT DataLink

Exemption

Clause 4 of the Proclamation establishing the Privacy Committee of South Australia provides that the Committee may exempt any person or body from one or more of the Information Privacy Principles[12] (IPPs) on such conditions as the Committee sees fit. The following exemption from the IPPs is granted.

This exemption applies to the Department for Families and Communities (DFC). It is an exemption from compliance with Principle 10, permitting DFC 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 and is limited to:

- Record identifier
- 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 including geocodes if available
- 85 File Number – 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.

The information disclosed to SA NT DataLink is to be used for the creation of master linkage keys as part of the establishment of the South Australian Northern Territory Data Linkage System (Data Linkage System) by the Data Linkage Unit within SA NT DataLink.

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 Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of DH within the Data Linkage Unit.

DFC remains responsible for the secure transfer of personal information in line with the Information Privacy Principles.

---

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

Destruction or retention of personal information

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

Expiry

This exemption will be reviewed by DFC and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

12 January 2010

Exemption

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

This exemption applies to the Department of Health (DH). It is an exemption from compliance with Principle 8, allowing DH 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 and is limited to:

- Record identifier
- 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 including geocodes if available
- 85 File Number – 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.

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

The information is to be used for the creation of master linkage keys as part of the establishment of the South Australian Northern Territory Data Linkage System (Data Linkage System) by the Data Linkage Unit within SA NT DataLink.

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 Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of DH within the Data Linkage Unit.

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

Destruction or retention of personal information

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

Expiry

This exemption will be reviewed by DH and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

12 January 2010

Exemption

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

This exemption applies to the Department of Education and Children's Services (DECS). It is an exemption from compliance with Principle 10, allowing DECS to disclose personal information to the Data Linkage Unit within SA NT DataLink.

The personal information to be disclosed is from the Department for Education and Children's Services Public Schools Enrolment Dataset and is limited to:

- Record Identifier
- Personal Identifier
- Names
- Date of Birth

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

- 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

The information disclosed to SA NT DataLink is to be used for the creation of master linkage keys as part of the establishment of the South Australian Northern Territory Data Linkage System (Data Linkage System) by the Data Linkage Unit within SA NT DataLink.

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 Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of the Department of Health (DH) within the Data Linkage Unit.

DECS remains responsible for the secure transfer of personal information in line with the Information Privacy Principles.

Destruction or retention of personal information

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

Expiry

This exemption will be reviewed by DECS and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

12 January 2010

Exemption

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

This exemption applies to the Department of Health (DH). It is an exemption from compliance with Principle 8, allowing DH 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 of Education and Children's Services 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

The information is to be used for the creation of master linkage keys as part of the establishment of the South Australian Northern Territory Data Linkage System (Data Linkage System) by the Data Linkage Unit within SA NT DataLink.

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 Data Linkage System. The exemption is provided on the condition that the personal information is only to be accessed by officers of DH within the Data Linkage Unit.

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

---

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

Destruction or retention of personal information

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

Expiry

This exemption will be reviewed by DH and the Privacy Committee three (3) years following its approval unless required earlier. An extension may be negotiated with the Privacy Committee if required.

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

12 January 2010