Government of South Australia

Privacy Committee
Of South Australia

Annual Statement of Activity of the Privacy Committee of South Australia

For the year ending 30 June 2017

Executive Officer
Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 464
ADELAIDE SA 5001
Phone (08) 8204 8792
privacy@sa.gov.au

Table of Contents

1 Year in Review

The Privacy Committee of South Australia (Privacy Committee) was established by proclamation in 1989 and has been responsible for overseeing the implementation and maintenance of the Information Privacy Principle Instruction (IPPI), which was approved by Cabinet in 1989.

The Privacy Committee has continued to promote privacy protection within government agencies within the context of a dramatically altered technological landscape in which personal information is used. In 1989 the internet was in its infancy and cyber-crime was barely known, information was primarily held in paper files, and a coordinated or joined up government was not the norm.

The *Australian Community Attitudes to Privacy Survey 2017* conducted by the Office of the Australian Information Commissioner shows that Australians are increasingly concerned about their privacy. Sixty-nine per cent of Australians say they are more concerned about their online privacy than they were five years ago. The survey revealed that while nearly half of Australians (46%) are comfortable with government agencies using their personal details for research or policy-making purposes, four in ten are not comfortable (40%), and the balance are still unsure. Further, one-third (34%) of the community is comfortable with the government sharing their personal information with other government agencies. However, only one in ten (10%) is comfortable with businesses sharing their information with other organisations.

Government agencies continue to embrace advancement in technologies, increased sharing of information and expansion of online service delivery. These advancements can intensify the risks to personal information. The willingness of citizens to accept new technologies is closely tied to their confidence in government agencies and other organisations to handle their personal information in a fair, secure and appropriate manner. The Privacy Committee has worked with agencies this year to increase awareness of the need for early assessment of the impact of government initiatives on personal information privacy so that solutions and protections can be built into the design of the project.

The Privacy Committee supports appropriate information sharing by the public sector and provided advice in relation to information sharing initiatives throughout the year. The importance of collaboration in addressing complex public policy issues and in providing better services to the community is well documented and supported. However, the relationship between privacy and information sharing has at times been misunderstood. Privacy has been cited as a reason to refuse to disclose personal information in circumstances where there is a clear permission within the IPPI that allows information to be shared for that purpose. It is vital that public sector agencies continue to improve their understanding of the personal information protections built into the IPPI.

It is equally important that information sharing is responsible and appropriate. Citizens are often compelled to engage with government agencies in order to receive services and benefits. Information sharing is essentially the repurposing of personal information, potentially moving away from the original purpose for which information was collected. The Privacy Committee continues to encourage agencies to be transparent about their information handling practices.

The Privacy Committee followed with interest the progress of the *Public Sector (Data Sharing) Act 2016* which passed through Parliament in December 2016. This Act

provides a legislative basis for government agencies to share information with each other and with entities outside of the South Australian Government. The Privacy Committee provided advice on the development of this legislation and the supporting regulations. The Privacy Committee notes that the legislation does not include personal information privacy protection safeguards.

The Privacy Committee continues to be concerned about the ability of the IPPI to provide an adequate framework for protecting personal information in South Australian government agencies. South Australia remains one of only two Australian jurisdictions without specific legislation to protect personal information in its public sector. The Privacy Committee notes that many citizens expect and assume a level of privacy protection that is not covered by South Australian law.

The Privacy Committee remains strongly committed to working with the Government to introduce information privacy law in South Australia to address existing and emerging challenges. Legislation would ensure the personal information of South Australian citizens that is held by the public sector is afforded privacy protections consistent with that in other Australian states and territories.

During 2016-17 the Privacy Committee continued to fulfil its role in receiving privacy complaints, responding to privacy enquiries and granting exemptions from the IPPI that it considered in the public interest. During the reporting year, the Privacy Committee extended or granted exemptions to South Australian Government agencies across eight subject areas and finalised ten complaints. The executive support to the Privacy Committee handled 77 enquiries from the public and 93 requests for advice from State Government agencies.

This is a report of the activities of the Privacy Committee for the year ending 30 June 2017.

Simon Froude

PRESIDING MEMBER

PRIVACY COMMITTEE OF SOUTH AUSTRALIA

2 South Australian Public Sector Privacy Framework

2.1 The Information Privacy Principles Instruction

South Australia's Information Privacy Principles Instruction (IPPI) was introduced in July 1989 by means of *Cabinet Administrative Instruction 1/89*, issued as *Premier & Cabinet Circular No. 12*. The IPPI includes a set of ten Information Privacy Principles (IPPs) that regulate the way South Australian public sector agencies collect, use, store and disclose personal information.

2.1.1 Information Privacy Principles

The IPPI can be accessed on the Department for the Premier and Cabinet website.

2.1.2 Amendments to the Information Privacy Principles Instruction

Two amendments to the IPPI came into operation in the reporting year. The IPPI Schedule was amended to include the Compulsory Third Party Regulator and the Judicial Conduct Commissioner as agencies to which the IPPI does not apply.

2.2 The Privacy Committee of South Australia

2.2.1 Establishment and Functions

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

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

A copy of the Proclamation can be found following the IPPI.

State Records of South Australia supports the Privacy Committee through the provision of executive support and advice, as well as the management of enquiries and complaints.

2.2.2 Privacy Enquiries

During the reporting year, State Records responded to 77 telephone and email enquiries from the public relating to all aspects of privacy of personal information.

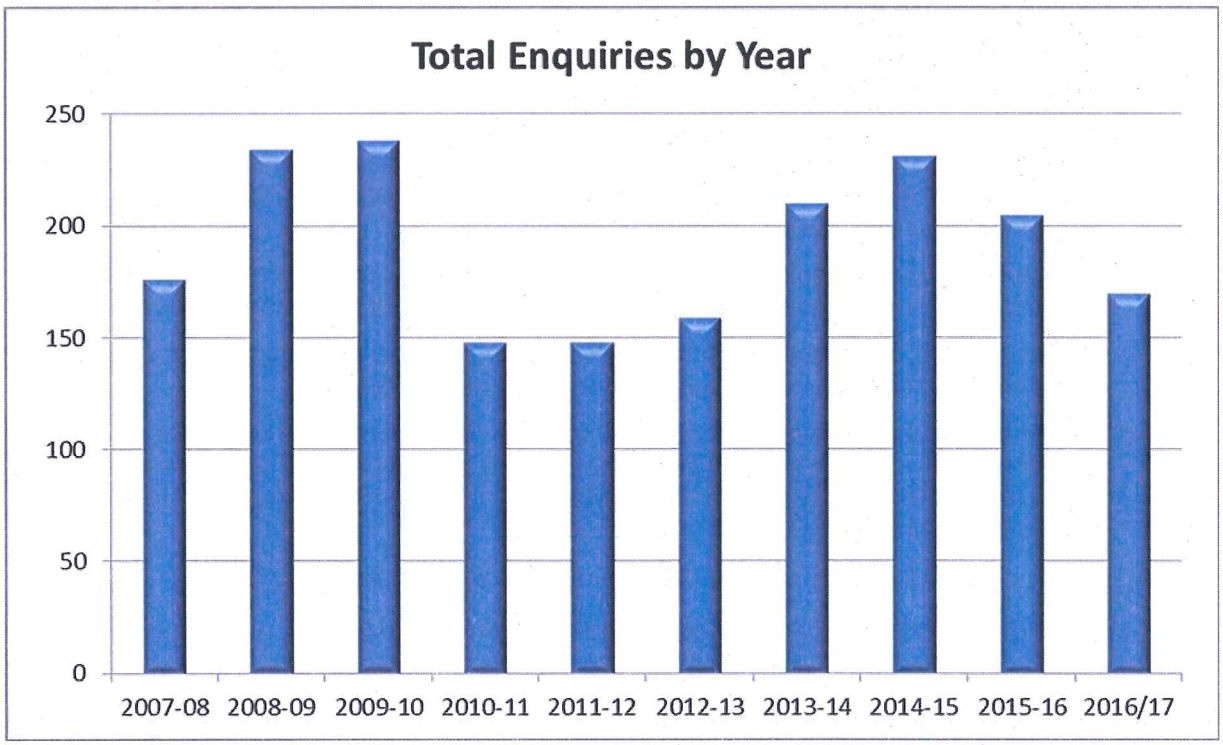
Common themes of public enquiries relate to:

- the use/disclosure of personal information obtained by SA government public sector agencies in relation to their employees
- the transfer of personal information to private organisations where a previously public service has been privatised
- matters concerning the use of listening and video surveillance devices.

State Records received 93 enquires/requests for advice from State Government agencies. Advice was provided across a broad range of personal information protection matters, including:

- protection of personal information in information sharing arrangements
- the impact of the *Public Sector (Data Sharing) Act 2016*
- content of privacy statements on agency websites
- binding contracted non-government parties to the IPPI
- the interaction of the IPPI and the *Freedom of Information Act 1991*.

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



Over the reporting year:

- 62 percent of all enquiries were dealt with over the telephone
- The number of enquiries received from the public decreased by 26 per cent from 104 in 2015-16 to 77 in 2016-17.
- The number of enquiries/requests for advice received from State Government agencies decreased by 8 per cent, from 101 in 2015-16 to 93 in 2016-17.

2.2.3 Meetings

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

2.2.4 Guidelines for members

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

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

2.2.5 South Australia's Strategic Plan

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

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

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

2.2.6 Seven Strategic Priorities

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

- creating a vibrant city;
- safe communities and healthy neighbourhoods;
- an affordable place to live;

- every chance for every child;
- growing advanced manufacturing;
- realising the benefits of the mining boom for all; and
- premium food and wine from our clean environment.

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

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

3 Activities of the Privacy Committee

3.1 Advice to the Minister

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

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

3.2 Public Sector (Data Sharing) Act 2016

The *Public Sector (Data Sharing) Act 2016* (the Act) passed the South Australian Parliament on 1 December 2016. The Act provides for the sharing of data between public sector agencies, and between public sector agencies and other entities.

Under the scheme of the Act, the sharing and use of public sector data is guided by five trusted access principles. Those principles are: safe projects, safe people, safe settings, safe output and safe data. The Act does not include a privacy safeguard.

The safe data principle provides that if the data to be shared and used contains personal information, the personal information must be de-identified unless one of seven criteria applies. Four of the seven criteria reflect the current exceptions in IPP10 (a) (b) (c) and (e). The other criteria where the personal information does not need to be de-identified before being shared, include:

- where the personal information is in connection with the wellbeing, welfare or protection of a child or other vulnerable person; and
- the purpose of the sharing cannot be achieved through the use of de-identified data and it would be impracticable in the circumstances to seek the consent of the person to whom the information relates.

The Committee provided advice to the Department of the Premier and Cabinet in relation to the Act and the regulations to support the Act. The Committee expressed its concern that the Act has the potential to erode the rights of individuals to have

their personal information handled by state agencies in a matter consistent with the IPPs.

The Act forms part of a broader data sharing reform program which includes the creation of a Data Sharing Committee. The functions of the Data Sharing Committee will include assessing requests regarding ethical approval, release of government held data and ensuring that data is protected and public confidence is maintained. The Presiding Member of the Privacy Committee has been nominated to be a member of the Data Sharing Committee.

3.3 Privacy Developments in other jurisdictions

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

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

The Commonwealth and each State and Territory Government within Australia, with the exception of Western Australia, has privacy legislation. These regimes are of interest to the Privacy Committee as it considers its own responses to local and national issues.

3.3.1 Australian Government

The *Privacy Amendment (Notifiable Data Breaches) Bill 2016* passed the Australian Parliament on 13 February 2017. It amended the *Privacy Act 1988* by introducing a mandatory data breach notification regime. The amendment requires government agencies, and businesses covered by the Privacy Act, to notify any individuals affected by a data breach that is likely to result in serious harm. It will also make it mandatory to advise the Office of the Information Commissioner of these serious breaches.

The *Privacy Amendment (Re-identification Offence) Bill 2016* was introduced to the Australian Parliament on 12 October 2016. The Bill aimed to amend the *Privacy Act 1988* to prohibit conduct related to the re-identification of de-identified personal information published or released by Commonwealth entities. The proposed changes would make it a criminal offence to re-identify government data that has been stripped of identifying makers. Publishing or communicating any re-identified dataset would similarly be considered a criminal offence.

3.3.2 Other States

Legislation was passed in the Victorian parliament this year to abolish the office of the Privacy and Data Protection Commissioner. The *Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017* establishes the Office of the Victorian Information Commissioner which will be responsible for the oversight of the *Privacy and Data Protection Act 2014* from 1 September 2017.

3.4 Recommendations and submissions

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

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

Pre-employment Declarations - Commissioner for Public Sector Employment (CPSE)

The Privacy Committee worked with the CPSE throughout the year in relation to the personal information protection issues arising in the development of a single Pre-Employment Declaration for South Australian Government agencies.

This issue was originally brought to the Privacy Committee's attention through a complaint about the collection of information concerning spent convictions.

On 5 October 2016 the CPSE released for consultation a draft Guideline on the Recruitment and Pre-employment Declaration Form. The Committee provided privacy advice in relation to:

- the timing of the collection of sensitive information such as criminal record information to avoid the unnecessary collection of personal information of those who apply for employment but do not get offered an interview
- information to be provided to applicants in relation to Spent Convictions
- the storage of highly sensitive personal information collected through the form
- privacy training to be provided to those who handle information collected through the form.

SA NT DataLink – Data Integration Unit

SA NT DataLink is an unincorporated joint venture comprising the South Australian and Northern Territory Governments and a number of non-government organisations and SA universities. SA NT DataLink enables the linkage of administrative and clinical datasets to allow population level health, social, education and economic research and evidence-based policy development to be undertaken with de-identified data, minimising risks to individual privacy when compared to traditional sample based research using identified data.

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

At its meeting on 12 October 2016, SA NT DataLink sought advice from the Privacy Committee in relation to the application of the 'separation principle". The separation principle involves a third party who separates the identifying information from other data. The identifying data is then provided to SA NT DataLink for linkage to other

approved data sets and once the project specific linkage keys have been attached, SA NT DataLink provides the identifying information and keys to the third party and other data custodians. They then extract the de-identified information and attach the linkage keys and make it available to the researchers.

SA NT DataLink advised the Privacy Committee that SA Health's Human Research Ethics Committee (HREC) responded recently to a paper provided to it by SA NT DataLink on the separation principle by agreeing that the use of a third party is desirable, but it also reserved the right to approve a data linkage project where it concludes that the separation principle is not required. SA NT DataLink were concerned that this could lead to a situation where SA NT DataLink is requested by a researcher and/or data custodian to approve linkage projects where the HREC has approved a project that does not fully comply with the separation principle.

SA NT DataLink advised the Privacy Committee that it strongly supports the separation principle and that public confidence in SA NT Data Link is based on the assurance that they will never release more information about individuals than is strictly required. A small number of projects (less than 10%) have sought an exemption from the separation principle for their particular proposal.

The Privacy Committee affirmed its preference for the separation principle to remain as it is best practice, and was satisfied with the governance process conducted by SA NT DataLink and noted that at times an exception to the separation principle would be justified.

Privatisation of Land Services Group

At its meeting on 12 October 2016, the Privacy Committee discussed the SA Government's announcement in the 2016-17 Budget that some of the transactional functions of the Land Services Group in the Department of Planning Transport and Infrastructure would be privatised. The Privacy Committee wrote to the cross-government reference group established to assist with the privatisation process and advised of its concerns for the ongoing protection of the personal information provided to any third parties outside of government. It advised of its view that a Privacy Impact Assessment should be conducted to assess and identify the impact the project might have on individuals, and set out recommendations for managing, minimising or eliminating their impact.

Trusted Digital Identity Framework

On 11 May 2017 the Executive Officer of the Privacy Committee attended a forum with the Australian Government Digital Transformation Agency and representatives from across the South Australian Government to discuss the connection of a South Australian digital identity to the beta National Digital Identity Exchange (the NDIE).

The NDIE aims to make it easier and faster for people to securely transact with government through digital channels. The Executive Officer gave a presentation to the forum on the requirements of the IPPI and some of the privacy challenges involved in the creation of a federated digital identity.

National Facial Biometric Matching Capability

On 15 June 2017 the Presiding Member and the Executive Officer met with officers from the Intelligence and Identity Security Division of the Commonwealth Attorney-General's Department (AGD) in relation to South Australia's participation in the National Facial Biometric Capability (the Capability). Discussion focussed on making South Australian driver licence images available for face matching through the National Driver Licence Facial Recognition Solution.

On 30 June 2017 the Presiding Member and the Executive Officer met with representatives from the Department of the Premier and Cabinet, SA Police, Department of Planning Transport and Infrastructure and the Attorney General's Department to discuss the privacy issues related to the project.

The sharing of this identity information will occur through the Document Verification Service, Face Verification Service, Face Identification Service, One Person One Licence Service and the Facial Recognition Analysis Utility Service.

The Face Verification Service (FVS) is a one-to-one image based verification service that can match a person's photo against an image on one of their government records, such as a licence photo, to verify their identity. The verification is facilitated by the interoperability hub which transmits queries and responses between agencies. The hub is not a database; it does not conduct biometric matching or store personal information. In relation to the FVS, many agencies requesting verification of an identity will receive a yes or no response to their request only. These transactions will mostly occur with the individual's consent.

A Face Identification Service (FIS) is expected to commence in 2018 to help determine the identity of unknown persons. It will be used for investigations of serious offences by specialist officers. Access to the FIS will be limited to police and security agencies, or specialist fraud prevention areas within agencies that issue passports, and immigration and citizenship documents. Police will only be able to use the FIS for investigations of more serious offences. Access to the FIS will only be provided to a limited number of users in specialist areas with training in how to interpret the results, to help guard against the potential for false matches.

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

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

During the reporting year the Privacy Committee did not make any public statements or publish public guidance on existing or emerging threats to individual privacy.

3.6 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'*.

3.6.1 Privacy Breaches

Northern Adelaide Local Health Network

In the previous reporting year the Privacy Committee was notified by the Northern Adelaide Local Health Network (NALHN) of a privacy breach concerning patient records of the Lyell McEwen Hospital. The Committee was advised that a member of the public had found clinical paperwork on the street. The paperwork included a copy of the Northern Area Midwifery Group Practice client list, student midwife names and phone numbers, and pathology results.

The Committee deferred consideration of the incident for State Records, in accordance with the *State Records Act 1997*, to undertake a survey of the record management practices of NAHLN. The results of this enquiry were presented to the Privacy Committee at its meeting on 1 March 2017. The survey did not reveal evidence to suggest that the incident was deliberate. The Privacy Committee was advised that in response to the incident, NALHN had taken the following actions:

- obligations of patient confidentiality has been added to the agenda at all staff forums
- a comprehensive review of the policy and procedural framework that references paper-based healthcare records and information security relating to patient information was undertaken to inform enhancements to the policy and procedural framework
- implementation of education and induction initiatives incorporating a communication strategy that reminds staff of their responsibilities to patient confidentiality
- commencement of a register of all processes related to the transfer and movement of paper-based healthcare/medical records and patient information within, around and across sites.

The Privacy Committee was satisfied that appropriate actions had been taken.

Northern Adelaide Local Health Network

In 2015 the Privacy Committee became aware through media reports that the son of a patient had found, amongst his late mother's belongings, copies of medical information of three other patients from the Lyell McEwin Hospital.

State Records commenced an investigation (survey) into this matter in March 2015 and provided a copy of its findings to the Privacy Committee which it considered at its meeting on 12 October 2016.

The Committee was advised that the State Records' survey did not reveal evidence to suggest the release was a deliberate act. The survey concluded that copies of clinical records (to assist with shift handover) were inadvertently bundled with copies of investigations that were given to the patient. Considering the Lyell McEwin Hospital had commenced reviewing its policies and procedures, including its handover procedure, State Records determined that no further action would be taken.

SA Health

In the last Annual Report of the Committee it was reported that the Privacy Committee had written to the Chief Executive of SA Health in February 2016 in relation to allegations that 21 staff had inappropriately accessed patient records in the previous year. The letter requested details of the results of an audit carried out by SA Health in to the alleged unauthorised access and an explanation of the steps taken to prevent unauthorised access to patient records in the future.

SA Health responded to the Privacy Committee by letter dated 19 October 2016. The letter advised that the following actions were taken as a result of the audit:

- an extensive review of the Incident Management and Open Disclosure polices has been undertaken and an updated toolkit has been provided to all staff
- the standard contract clause around confidentiality has been reviewed and will progressively be applied to all new contracts
- SA Health will be undertaking a more in-depth review of its identity and access management arrangements, given the progressive roll-out of the Chris 21 payroll system, which will consolidate all SA Health staff on one database and allow for a better platform to manage the risks associated with user accounts.

SA Health has also implemented the following process improvements:

- a co-ordinated whole of Health approach to reporting and recording of privacy breaches
- research to determine better practice models for controls, auditing, and managing access to IT systems
- improved processes with the Security Services contractor to reduce the possibility of contract security staff having access to patient information
- the CE of SA Health determined that, subject to proper investigation affording all parties natural justice, the penalty for inappropriate access to patient information will be dismissal
- consideration has been given to possible amendments to the confidentiality provisions of the *Health Care Act 2008*
- staff awareness around privacy of patient information, the consequences for breaching privacy and open disclosure has been increased via internal communication, emphasis at staff orientation programs, a new clause added to role descriptions, the topic included in leadership training courses and generally via promotion by leadership
- Human Resources policies have been updated to highlight the importance of privacy of patient information and the consequences of breaching that privacy
- new protocols are being developed for dealing with allegations and investigations of inappropriate access to patient information
- on-line mandatory training for open disclosure and incident reporting is being developed as well as mandatory training covering privacy

- a newly developed quarterly community report originally planned to provide privacy breach statistics in context with whole of Health information will now be refocussed as a generic community report.

The Privacy Committee was satisfied with the actions taken.

TAFE SA

On 24 March 2017 TAFE SA reported to the Privacy Committee that an email was sent by a staff member to approximately 200 students with recipients receiving the names, email addresses and student ID numbers of all other recipients.

An internal investigation was being undertaken and the results will be provided to the Privacy Committee for consideration.

Office of the Director of Public Prosecutions

On 6 April 2017 the Office of the Director of Public Prosecutions reported to the Privacy Committee that on 1 April 2017 its website was subject to a malicious attack. This attack resulted in the repository of 167 student applications, including Curriculum Vitaes, covering letters and student university transcripts, being made available publically.

The Privacy Committee provided advice on dealing with the breach and the Committee was advised that all affected persons were notified by mail of the incident.

The agency has commenced an internal review of the event and the results will be provided to the Privacy Committee.

3.7 Complaints

The Privacy Committee has the function, under clause 2(g) of the Proclamation, *'to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority'*.

In the first instance, the Privacy Committee will generally forward complaints it has received to the agency concerned and seek the agency's opinion on what took place and what action has been or might be taken to resolve the matter. The Committee will then assess the response and, if necessary, make a recommendation to the agency to amend its practices or to adopt other measures to resolve the complaint. The Privacy Committee may also refer the complainant to the South Australian Ombudsman if it remains dissatisfied with the agency's response.

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

At the start of the reporting period the Committee had three open complaints. The Committee received eight complaints in the reporting year. The Committee finalised ten complaints.

3.7.1 Complaints Concluded Summary Table

Respondent Organisation	Information Privacy Principle (IPP)	Outcome
Government Department	IPP 10 – Disclosure of personal information to third party	No breach of the IPPI
Government Department	IPP 10 – Disclosure of personal information to third party	Breach of the IPPI referred to agency for action
Tribunal	IPP 10 – Disclosure of personal information to third party	IPPI not applicable
Government Department	IPP 10 – Disclosure of personal information to third party	Committee declined to accept complaint on the basis it had previously been considered by an external complaint authority
Government Department	IPP 3 –Collection of irrelevant personal information	Breach of the IPPI referred to agency for action
Government Department and Independent Statutory Authority	IPP 10 – Disclosure of personal information to third party	No breach of the IPPI
Government Department	IPP 10 – Disclosure of personal information to third party	Complaint from employee of Crown in relation to their employment
Minister	IPP 10 - Disclosure of personal information to third party	No breach of the IPPI
Government Department	IPP 10 - Disclosure of personal information to third party	No breach of the IPPI
Government Department	IPP 10 - Disclosure of personal information to third party	Committee declined to accept complaint on the basis it had previously been considered by an external complaint authority
Statutory Corporation	IPP 10 - Disclosure of personal information to third party	Breach of the IPPI referred to agency for action

3.8 Exemptions

The Privacy Committee may, under clause 4 of the Proclamation, *'exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Privacy Committee thinks fit'*.

Requests for exemptions are considered on a case-by-case basis. Exemptions are only applied in situations where the Privacy Committee considers that the public interest for an activity outweighs the privacy protections afforded by the IPPI, or where otherwise warranted by unique circumstances. Exemptions are generally subject to conditions, such as an expiry date, an approval from an appropriate research ethics committee, or a requirement for the agency to report on the activity conducted under the exemption.

The Privacy Committee granted exemptions across eight subject areas throughout the reporting year. The full exemptions are available in the Annual Report of the Privacy Committee and on the State Records' website.