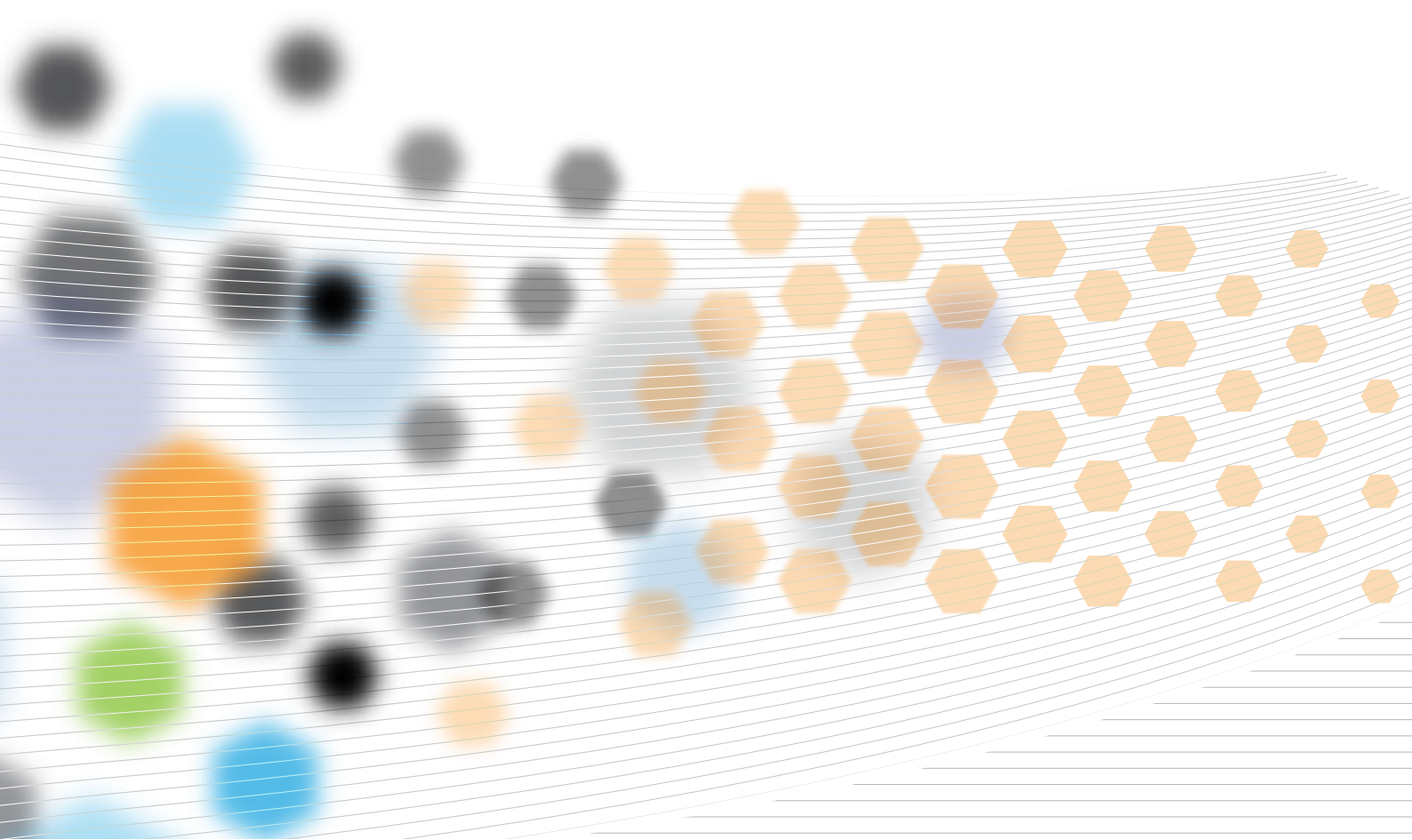


Commissioner for Privacy and Data Protection

Annual Report 2015–16




The Hon. Gavin Jennings MLC
Special Minister of State
Level 1, 1 Treasury Place
EAST MELBOURNE VIC 3002

Dear Minister

ANNUAL REPORT

I am pleased to present you with the Annual Report for 2015-16 in accordance with Part 6 section 116 (1) of the *Privacy and Data Protection Act 2014*, for presentation to Parliament.

Yours sincerely



DAVID WATTS
Commissioner for Privacy and Data Protection

Commissioner for Privacy and Data Protection

Annual Report 2015–16

Contents

Commissioner's Overview	8
The role of the Commissioner for Privacy and Data Protection	10
The objectives of the Commissioner for Privacy and Data Protection	11
Operational Privacy and Assurance	12
Information Privacy Enquiries and Complaints	13
Complaints handling review	17
Breach Notifications	17
Voter Information – Public Interest Determinations	17
Submissions to Government	17
Privacy Complaint at the Supreme Court of Victoria	18
Strategic Privacy	20
Privacy policy – Modernising privacy	20
Privacy by Design	20
Information sharing	21
Royal Commission into Family Violence	21
New technology	22
Tools and resources	23
Flexibility mechanisms	23
Data Protection	24
Valuing Public Sector Data	24
What is the Victorian Protective Data Security Framework?	25
The principles	26
The standards	26
The assurance model	27
Resources	27
Law Enforcement Data Security	28
Crime Statistics Agency	28
Victoria Police	28
Privacy and Data Protection Networks	36
Youth Advisory Group	36
Inter-agency Privacy Officers' Forum	36
Privacy and Data Protection Week	36
Privacy Authorities Australia	37
Asia Pacific Privacy Authorities	37
Global Privacy Enforcement Network	37
UN Global Pulse	37
All-States Data Security Group	37
About the Office of the Commissioner for Privacy and Data Protection	38
Organisational Structure and Staffing	39
Governance and Reporting	40
Shared Services	40
Communications and Publications	40
Occupational Health and Safety	41
Workplace Relations	41
Public Sector Conduct	41
Environmental Impacts	41
Risk and Insurance Management	41
Freedom of Information	41
Consultancies	42
Information and Communication Technology Expenditure	43
Overseas Travel	43
Major Contracts	43
Protected Disclosures	43
Gifts, Benefits and Hospitality	43
Statement of Availability of Other Information	43
Annual Financial Statements 2015-16	44
Appendix A – Disclosure Index	75
Appendix B – Attestation Complying with Standing Direction 4.5.5	77
Appendix C – Budget Paper 3	78



Commissioner's Overview

At the date of preparing this annual report, legislation is before Parliament that abolishes this office. Assuming that the legislation is passed, this will be our second and final annual report.

In these circumstances, I think that it is important to highlight the major things we have achieved in less than two years:

- development of the Victorian Protective Data Security Framework and Victorian Protective Data Security Standards
- development and implementation of the Crime Statistics Agency Data Security Standards
- introduction of mobile 'apps' for CPDP and Victorian public sector Business Impact Levels
- development and implementation of the first Information Usage Arrangement and Certification under the new State privacy flexibility mechanisms
- finalisation of the 6 year longitudinal survey of Victoria Police information security culture
- thought leadership through papers and presentations on the privacy implications of emerging technologies, including big data, cloud computing, biometrics, identity management, de-identification and smart cities
- development of a 30 page guidance document for the Victorian public sector on appropriate Information sharing practices, including an interactive PDF

- design and rollout of a free online privacy training module for the Victorian public sector
- review of processes for handling privacy complaints by members of the public
- an intense program of stakeholder consultation and engagement
- participation in a broad range of national and international privacy and data security forums

The work we have done has transformed the way that privacy and data security are perceived. No longer is either considered to impede innovation or service delivery transformation in the Victorian community.

This long overdue reconceptualisation of privacy and data security has been undertaken by an office staff of about twenty dedicated and highly motivated people. I take this opportunity to thank them for their dedication, tirelessness and sense of humour.

Our work has also been undertaken in an environment where no additional funding was allocated by government to finance our significantly expanded role.

This office has laid the foundation for information reform within the Victorian public sector. I am proud to have had the good fortune to lead it through the challenges it has faced and overcome.



David Watts

Commissioner for Privacy and Data Protection



The role of the Commissioner for Privacy and Data Protection

The *Privacy and Data Protection Act* came into effect on 17 September 2014. It repealed the *Information Privacy Act 2000* and the *Commissioner for Law Enforcement Data Security Act 2005*, but combined those regulatory functions in the one piece of legislation.

In addition it: introduced new privacy flexibility mechanisms that permit departures from the Information Privacy Principles if there is a substantial public interest in doing so, and; established a legislative basis for the development of a protective data security framework across the Victorian public sector.

The purposes of the *Privacy and Data Protection Act 2014* are principally:

- to provide for responsible collection and handling of personal information in the Victorian public sector
- to provide remedies for interference with the information privacy of an individual
- to establish a protective data security regime for the Victorian public sector
- to establish a regime for monitoring and assuring public sector data security

The Commissioner for Privacy and Data Protection has a number of legislated functions. For information privacy, they are principally:

- to promote an understanding and acceptance of the Information Privacy Principles (IPPs) and their objectives

- to develop and approve codes of practice
- to publish model terms capable of being adopted in a contract or arrangement with a recipient of personal information
- to examine practices, including the conduct of audits, to ascertain compliance with the IPPs
- to receive and handle information privacy complaints
- to issue compliance notices and carry out investigations
- to review proposed legislation with regard to its impact on information privacy
- to consult and cooperate with persons or organisations concerned with information privacy and make public statements regarding information privacy
- to issue guidelines and other material with regard to the IPPs
- to carry out information privacy related research



For protective data security and law enforcement data security, they are principally:

- to issue protective data security standards and law enforcement data security standards and promote their uptake
- to develop the Victorian protective data security framework
- to conduct monitoring and assurance activities to ascertain compliance with data security standards
- to issue guidelines and other material with regard to protective data security standards
- to carry out data security related research

The Commissioner for Privacy and Data Protection also exercises a number of powers, notably:

- to require access to data and data systems from public sector body heads and the Chief Commissioner of Police
- to request access to crime statistics data
- to make public interest determinations with regard to information privacy arrangements
- to approve information usage arrangements
- to certify the consistency of an act or practice with the IPPs
- to issue information privacy compliance notices
- to examine witnesses

The jurisdiction of the Commissioner extends to public sector agencies with regard to protective data security and public sector agencies and local government with regard to information privacy. The Commissioner's jurisdiction extends also to contractors providing services under a State contract which binds the service provider to adherence to the IPPs.

The objectives of the Commissioner for Privacy and Data Protection

The Commissioner's objectives form the basis of a three year strategic plan established in 2014. A number of key activities and projects are directly related to and support the achievement of these objectives.

The Commissioner's objectives are to:

- build information privacy and data security capability, resilience and assurance across the Victorian public sector
- enable privacy-respectful and secure information sharing practices for the public interest
- encourage public sector agencies and citizens to share responsibility for data protection
- enable new technologies through implementing Privacy by Design and Security by Design
- provide privacy and data security thought leadership
- contribute to the development of public value across the Victorian public sector.



Operational Privacy and Assurance

Since the creation of CPDP in September 2014, the Operational Privacy and Assurance Branch has made a number of significant achievements.

Highlights include:

- 2,924 enquiries resolved
- 65 complaints handled
- 40 voluntary privacy breach notifications received
- assisted the Commissioner with his participation in a privacy complaint before the Supreme Court of Victoria
- a new case management system implemented
- commissioned and participated in an independent review of the assurance complaint handling process
- made submissions to State Government on the eight-year review of the *Charter of Human Rights and Responsibilities Act 2006*, the Royal Commission into Family Violence and on the issue of Fuel Drive Offs
- made a submission to the Commonwealth Government on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* and participated in consultation on the Commonwealth Royal Commission into Institutional Responses to Child Sexual Abuse
- undertook two formal consultations with the Victorian Electoral Commission following requests from applicants for access to the electoral roll
- held a number of general consultations with a wide range of stakeholders relating to operational privacy issues and projects
- reviewed various local councils' privacy policies and provided commentary
- produced an online 'how to make a complaint' video and introduced a secure electronic complaint lodgement facility
- revised and updated information for complainants and respondents with respect to the complaint handling process
- re-established, coordinated and chaired five meetings of the Youth Advisory Group, including hosting an event for the 2016 Privacy and Data Protection Week – *Privacy: Who cares?*
- established, coordinated and chaired quarterly meetings of the Inter-Agency Privacy Officers' Forum

Operational Privacy and Assurance Branch's achievements for the reporting period 1 July 2015 until 30 June 2016 (the reporting period) are explained in further detail below.

Information Privacy Enquiries and Complaints

CPDP received 1,488 enquiries from the general public and from staff of organisations regulated by the *Privacy and Data Protection Act 2014* during the reporting period.

Section 13 of the *Privacy and Data Protection Act 2014* sets out who has obligations under the Act. Typically, these relate to Victorian government organisations, local councils and contracted service providers working under a state contract.

Of the 1,488 enquiries received, 48% were within the jurisdiction of the CPDP. Enquiries that fell outside the jurisdiction of the CPDP were referred to the appropriate organisation, typically the Office of the Australian Information Commissioner (for enquiries regarding Commonwealth organisations or some private sector organisations), the Health Services Commissioner (for enquiries regarding health information) and Victoria Police (for enquiries regarding the use of Closed Circuit Television (CCTV)).

Consistent with the 2014/15 reporting period, the Information Privacy Principles (IPPs) most commonly raised by enquiries within the CPDP's jurisdiction related to:

- IPP 1 (collection)
- IPP 2 (use and disclosure)
- IPP 4 (data security).

Common enquiry themes included:

- disclosure of personal information from one organisation to another organisation
- use of CCTV in the workplaces and public areas
- the interpretation of the IPPs
- the taking and publication of photographs of individuals
- online publication of personal information.

The Complaint Handling Process

Many enquirers sought information on how to make a privacy complaint. To assist potential complainants with the complaints process, a short animated video on 'How to make a privacy complaint' was published on the CPDP website.



If an enquiry falls within jurisdiction, the individual is requested to refer the potential complaint to the organisation in question as the first step. Doing so affords procedural fairness and meets the Commissioner's obligation to give an organisation adequate opportunity to address a matter before formal involvement by the CPDP.

If the individual is not satisfied with the outcome of that first step, step two involves a formal assessment to determine if the enquiry constitutes a complaint. The Commissioner considers whether the enquiry:

- involves an organisation within the jurisdiction of the *Privacy and Data Protection Act 2014*
- involves personal information
- raises one or more of the IPPs.

Once an enquiry has been accepted as a complaint, the Commissioner contacts the organisation against which the complaint is directed to request a formal response. Upon receipt of the response and discussion with the complainant, the Commissioner will decide to either:

- decline to entertain the complaint further
- not decline the complaint, but consider if conciliation by the CPDP is inappropriate
- not decline the complaint and refer it to conciliation by the CPDP, if he believes that a complaint may be conciliated successfully. To reach that decision, the Commissioner has regard to the complexity of the complaint, the parties involved, the relationship between the parties, their attitudes and willingness to participate in conciliation, and outcomes sought.

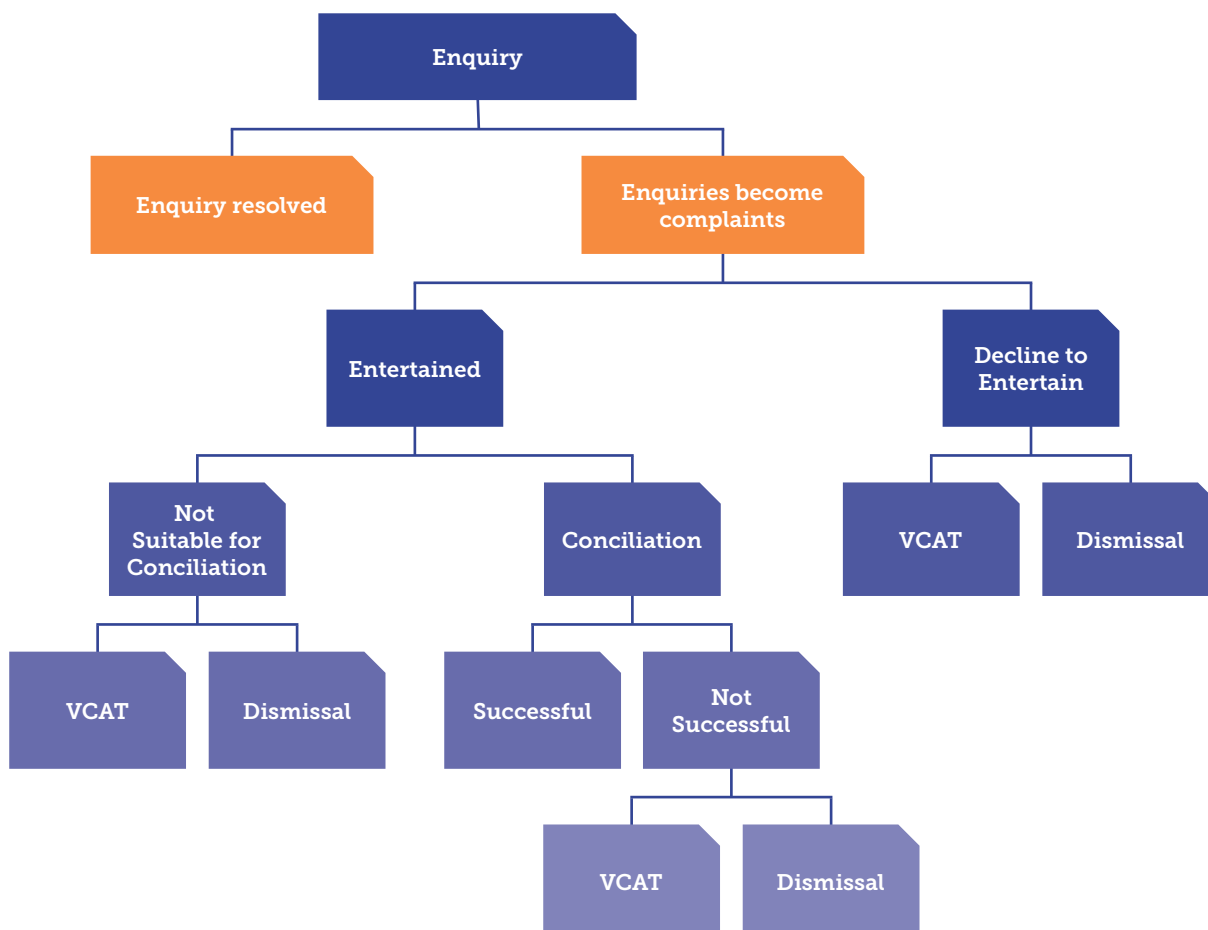
Conciliation is similar to mediation, and is a form of alternative dispute resolution. CPDP conducts the process and remains neutral throughout. The purpose of conciliation is to give the parties an opportunity to discuss the complaint and see if they can reach a mutually agreeable resolution.

Where the Commissioner has declined to entertain a complaint, considered that conciliation is inappropriate or if conciliation has failed, he will notify the complainant that they have the right to request him to refer the complaint to the Victorian Civil and Administrative Tribunal (VCAT).

For the purpose of recording and reporting outcomes, a complaint is considered to be closed in a number of situations, including where:

- a complaint is declined, is not referred to VCAT and is then dismissed
- a complaint is not declined, not referred to conciliation and referred onto VCAT
- a complaint is not declined, but is referred to conciliation and settles
- a complaint is not declined, referred to conciliation, but does not settle, the complainant does not request the office to refer it to VCAT and the complaint is dismissed.

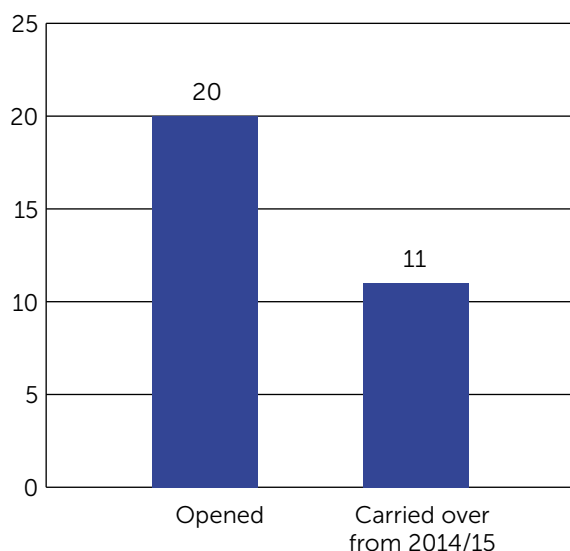
Outline of the Complaints Handling Process



Complaint outcomes

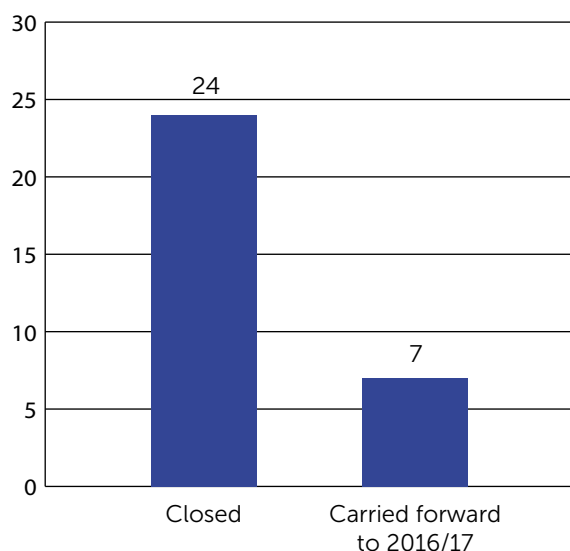
Thirty-one complaints were handled during the reporting period. This included 11 complaints that were carried over from the 2014/15 period and 20 new complaints received during the reporting period.

Total complaints 2015/16



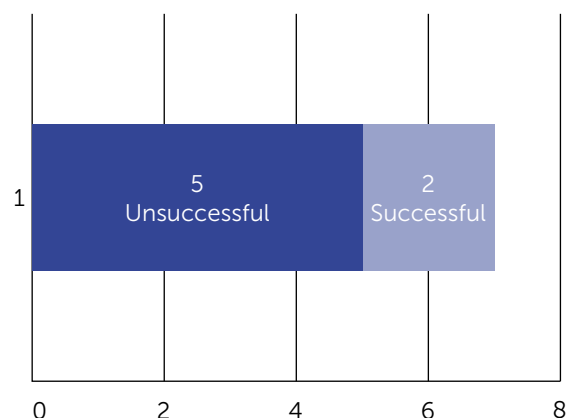
Twenty-four complaints were investigated and closed during this period, with seven complaints carried over to 2016/17.

Complaint status 30 June 2016



During the reporting period, seven complaints proceeded to conciliation. Of these, two were successfully conciliated, with five conciliations being unsuccessful.

Conciliation outcomes 2015/16



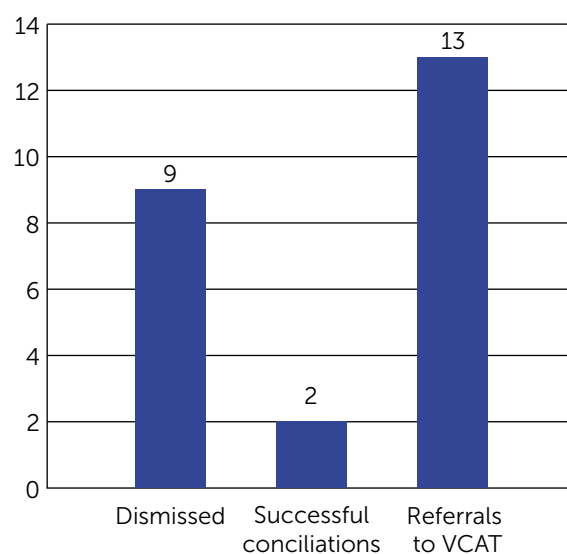
Typical outcomes of conciliation at CPDP may include:

- an apology to the complainant, and/or
- agreement by the respondent to provide privacy training to staff and/or review its own privacy policies and procedures.

In cases where a complaint is declined to be entertained, where conciliation fails, or where the Commissioner determines that it is not reasonably possible to conciliate the complaint, complainants are advised of their right to request that the Commissioner refers the complaint to VCAT.

Thirteen cases were referred to VCAT during the reporting period.

Complaint outcomes 2015/16



Examples

The following table gives examples of some of the enquiries and complaints handled during the reporting period and their outcomes.

Issue	Outcome
An individual contacted the office concerned that a real estate agent had captured and published online photographs of the interior of their rental property for the purpose of selling the property. The photographs contained identifying information about the caller's family.	The caller was advised that a real estate agency, being a private company, was likely to be regulated by the <i>Privacy Act 1988</i> administered by the Office of the Australian Information Commissioner (OAIC). The caller was provided with the OAIC's contact details.
A staff member of a Victorian government organisation called the office concerned that their name had been included in an Honour Roll by their employer without their knowledge or permission.	As the matter fell within jurisdiction and potentially raised issues under IPP 2 (use and disclosure), the staff member was referred to the organisation's privacy officer, with a pathway back to this office should further assistance be required. During the conversation, the requirements of IPP 2 and the complaints process were briefly outlined.
A patient of a public hospital emailed the office seeking advice on how to access their medical records.	The enquirer was referred to the Office of the Health Services Commissioner, as it regulates health information in accordance with the <i>Health Records Act 2001</i> .
An individual alleged that a Council disclosed their personal information within the organisation in circumstances that they were advised would not occur. The individual had asked the Council to remain anonymous at the time their personal information was collected. The complaint brought IPP 1 (collection), IPP 2 (use and disclosure), IPP 4 (data security) and IPP 8 (anonymity) into question.	The Council investigated the complaint. It apologised to the individual for disclosing the personal information and not allowing the individual to remain anonymous. It spoke to staff members involved to remind them of their privacy obligations under the <i>Privacy and Data Protection Act</i> and the organisation's privacy policy. It noted that the organisation's induction program for new employees includes online training in relation to privacy legislation and the organisation's privacy policy. The Commissioner found that the Council had adequately dealt with the matter and elected to decline the complaint. The individual was advised of their right to request this office in writing to refer the matter to VCAT in accordance with the <i>Privacy and Data Protection Act</i> , but did not exercise that right. The complaint was subsequently dismissed and closed.
An individual alleged that an organisation disclosed their personal information to an unauthorised third party by sending their personal information to a third party email address. The complaint brought IPP 2 (use and disclosure), IPP 3 (data quality) and IPP 4 (data security) into question.	The organisation investigated the complaint and apologised for the disclosure. However, the Commissioner did not believe that the response adequately dealt with the complaint and found no grounds to decline it. The complaint was referred to conciliation, as both parties expressed a willingness to participate in the process. The complaint was successfully conciliated, and the Respondent agreed to pay the Complainant compensation (amount undisclosed). The Complainant advised the CPDP that no further action from the CPDP was required. The complaint was subsequently closed.
An individual was employed by an organisation covered by the <i>Privacy and Data Protection Act</i> . The individual alleged that the organisation disclosed their personal information relating to an employment matter to their colleagues for an unauthorised purpose. The complaint raised IPP 2 (use and disclosure) and IPP 4 (data security).	The Commissioner was unable to conclude that the response from the organisation adequately dealt with part of the complaint. This part of the complaint was referred to conciliation but the parties were unable to reach a mutually agreeable outcome. The individual exercised their right to request this office to refer the matter to VCAT. The complaint was subsequently closed.

Complaints handling review

During the reporting period CPDP's information privacy complaints handling process was reviewed. The aim of the review was to ensure that:

- all legislative requirements under the *Privacy and Data Protection Act* are met in a timely, efficient and effective way
- opportunities for improving and streamlining the process are identified
- trends in complaints are identified and used to inform our privacy policy work.

While the review was not finalised by 30 June 2016, interim measures recommended include internal enhancements to the complaint handling process and CPDP's electronic case management system. Recommendations from the review will be implemented during 2016-17.

Breach Notifications

Although not mandatory under the *Privacy and Data Protection Act*, public sector organisations are encouraged to notify the Commissioner if they believe they have breached one or more of the IPPs. Voluntary disclosure allows CPDP to provide appropriate information and guidance to the affected organisation, helps us to resolve complaints and demonstrates public sector commitment to transparent and accountable privacy practices.

During the reporting period, the Commissioner received 27 breach notifications, more than double the number of notification received during 2014-15.

Notably, one third of notified breaches involved email communications. Other breach notifications received during this period related to:

- personal information being published online in error
- third party theft of computers and phones
- employee theft
- documents containing personal information being misplaced on public transport
- account information being provided to the wrong customer
- inappropriate/insecure records disposal.

Voter Information – Public Interest Determinations

Under section 34 of the *Electoral Act 2002*, individuals and organisations may request the Victorian Electoral Commission (VEC) to provide access to electoral roll information. The VEC may only provide access where it has made a finding that the public interest in providing the requested information outweighs the public interest in protecting the privacy of personal information. The VEC is required to consult CPDP on the public interest in protecting the privacy of personal information, and take CPDP advice into account in making its decision.

During 2015-16, CPDP worked with the VEC to streamline the process for assessing the privacy and security aspects of these requests. We received two requests from VEC during 2015-16. The Commissioner assessed the public interest in the requests, including the procedures in place to ensure the privacy and security of the personal information provided. In one matter, the Commissioner advised the VEC to request further information, including a Privacy Impact Assessment and a Security Risk Assessment. In the second matter, the Commissioner advised the VEC that he was of the view that there was significant public interest in providing the information, and that this outweighed the public interest in protecting the privacy of personal information.

Submissions to Government

Inquiry into Fuel Drive Offs

In July 2015, CPDP made a submission to the Victorian Parliament's Law Reform, Road and Community Safety Committee in relation to its Inquiry into Fuel Drive Offs. Fuel drive offs are instances in which a person refuels a vehicle and drives off without paying. It is a persistent issue in Victoria.

In its submission, CPDP noted that 'measures may be introduced that offer a method in which petrol station operators or their agents [could] directly obtain from VicRoads the personal information of vehicle owners'. CPDP's view was that under current Victorian legislation 'it is unlikely that these provisions would allow sharing of Victorian Government data, such as registration data held by VicRoads'.

Further, 'if legislation were enacted to provide for the registration data to be given to private individuals or bodies, the very considerable privacy and data protection implications would need to be closely considered'.

Review of the Charter of Human Rights and Responsibilities Act 2006

CPDP contributed to the *Eight-year Review of the Charter of Human Rights and Responsibilities Act 2006* (the Charter). CPDP supported the terms of reference of the review, which make clear that it focused on ways to enhance the effectiveness of the Victorian Charter.

Article 13 of the Charter provides a multi-dimensional right to privacy and reputation in Victoria, including a right for an individual '(a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and (b) not to have his or her reputation unlawfully attacked'. The Charter right to privacy includes the protection of personal information but also encompasses bodily, territorial, communications and locational privacy.

CPDP's submission included a number of recommendations for enhancing the effectiveness of the Charter. These included proposing that consideration be given for the Charter to include a separate, stand-alone cause of action for violation of human rights, consideration for including alternative dispute resolution as the first level of redress in any remedies provision (as is the case with the *Privacy and Data Protection Act*), and the amendment of confidentiality provisions in the *Ombudsman Act 1976* and *Equal Opportunity Act 2010* to facilitate information sharing in relation to statutory functions under the Charter, where appropriate.

Privacy Complaint at the Supreme Court of Victoria

In 2013, CPDP received a complaint regarding the handling of personal information by a Contracted Service Provider (CSP), who was providing services to a Victorian Government Department under a State Contract, and who was bound by the *Privacy and Data Protection Act*. The complainants made complaints against both the Department and the CSP on behalf of themselves, and their children. The complainants alleged that the CSP had collected their personal information from the Department and disclosed their personal information to a third party in a way which contravened IPPs 1, 2 and 4, and that as a result of the disclosure, detrimental familial consequences ensued.

The Commissioner accepted the complaints for consideration. Following the Respondent's response, the Commissioner found no reasons to decline the complaints. However, given the factual complexity of the complaints, the number of parties involved (some of which were represented by lawyers and financial administrators), and the outcomes sought, the Commissioner decided that the complaints were not suitable for conciliation. The complainants asked the Office to refer the complaints to VCAT for hearing and in 2014, the case against the CSP proceeded to a final hearing.

VCAT found that although the alleged disclosure occurred, it did not constitute an interference with privacy. The complainants then sought leave from VCAT to appeal its decision in relation to IPP 4 (data security). This principle states that an organisation must take all reasonable steps to protect the personal information it holds from misuse and from unauthorised access, modification or disclosure. VCAT granted leave to appeal on this basis.

The complainants subsequently made an application to the Supreme Court of Victoria, to appeal VCAT's decision in relation to IPP 4. The Commissioner then made an application to the Supreme Court to intervene in the proceedings as a defendant, or if unsuccessful in that application, he sought to intervene in the proceedings as a "friend of the court". The Commissioner's position was that the Court could not properly construe the meaning of IPP 4, without having regard to IPP 1.

IPP 1 relates to the collection of personal information. IPP 1.3 states that at or before the time (or as soon as practicable thereafter) an organisation collects personal information about an individual, it must make the individual aware of certain matters. Particularly, of relevance to this complaint was IPP 1.3(d) which states that an organisation must make an individual aware of, "to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind". Moreover, IPP 1.5 states that "if an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual."

The complainants alleged that they were not advised by the CSP that it had collected their personal information from the Department, which it then shared with a third party, and providing notice as required by IPP 1.5 would not have posed a threat to the life or health of any individual. They alleged that a flow-on effect of this was that IPP 4 had been breached, because the disclosure of personal information was 'misused' and 'unauthorised access and disclosure' had occurred.

During the hearing, the Commissioner withdrew his application to intervene as the Court indicated that it would only consider arguments about IPP 4, and would not consider arguments relating to IPP 1 (although relevant). The complainants subsequently withdrew their application and the proceedings were dismissed, with no orders made as to legal costs.



Strategic Privacy

Privacy policy – Modernising privacy

The Strategic Privacy team within CPDP is responsible for leading the office's privacy policy work. The team supports the work of the Commissioner by conducting research into emerging areas of privacy, producing guidance materials, and supporting the Victorian public sector in meeting its privacy obligations under the *Privacy and Data Protection Act 2014*. In particular, the Strategic Privacy branch supports the Commissioner's function "to promote an understanding and acceptance of the Information Privacy Principles and of the objects of those Principles" under section 103(1)(a) of the *Privacy and Data Protection Act 2014*.

An underlying theme across the work of the Strategic Privacy team is the modernisation of privacy. As new technologies emerge and the public sector expresses interest in using them, guidance needs to be provided to organisations on how they can utilise and benefit from these technologies, while at the same time complying with the Information Privacy Principles (IPPs) under the *Privacy and Data Protection Act 2014*.

Privacy by Design

The Commissioner has continued to work towards implementing Privacy by Design (PbD) across the Victorian public sector. CPDP regularly consults with organisations that are developing initiatives involving personal information, to assist them to meet their privacy obligations under the *Privacy and Data Protection Act 2014*. Consultations range from general discussions with organisations in the early stages of a project, to working on specific solutions to enhance privacy as projects develop. Some of the common themes that CPDP has been engaged in include information sharing (with particular focus on whether the *Privacy and Data Protection Act 2014* permits information to be shared), web analytics, data linkage, and the delivery of services through online channels.

CPDP has also been asked to review six privacy impact assessments (PIAs) during the reporting period. The office has found that there has been increased uptake of the modernised PIA template released during the previous reporting period, which demonstrates that organisations are engaging with privacy early on in their initiatives.

CPDP has completed six PIAs relating to internal office projects. The PIAs cover the process for receiving and managing privacy complaints, and the use of instant messaging tools within the office, CPDP's use of Twitter, and its bring your own device program, among others. Two of these PIAs – relating to instant messaging and Twitter – will go on to inform new guidance material for the wider Victorian public sector, and the PIAs will be made available as examples on the CPDP website for other organisations to use.

Information sharing

Information sharing has continued to be an important topic guiding the work of CPDP over the reporting period. The Strategic Privacy team, along with the Commissioner, has consulted with a number of organisations on their proposed information sharing initiatives, and provided guidance on how they can share personal information within the bounds of the *Privacy and Data Protection Act 2014*. These consultations have revealed that many organisations either perceive privacy law to be a barrier to information sharing and therefore do not share information (even where authorised by law) or conversely, share information without regard to legislative restrictions.

In response to this, the Commissioner has worked hard to improve the public sector's understanding of the barriers to information sharing, which extend beyond the *Privacy and Data Protection Act 2014*. Following on from an information sharing checklist produced in the last reporting period, comprehensive *Guidelines for sharing personal information* – taking into account information privacy, protective data security and recordkeeping considerations – were released in March 2016. As a product of public sector consultations on this document, it became clear that a practical tool would further assist organisations in understanding their obligations under the *Privacy and Data Protection Act 2014*. To accompany the guidelines, CPDP produced an interactive online PDF that walks a user through the necessary questions they need to consider before embarking on information sharing initiatives.

To further promote a culture of responsible information sharing in the Victorian public sector, the Strategic Privacy and Data Protection branches jointly delivered three training sessions on information sharing as part of Privacy and Data Protection Week (PDP Week) 2016, reaching out to public sector staff in Melbourne and country Victoria. The Assistant Commissioner for Strategic Privacy has also presented on information sharing on numerous occasions, including at the Asia Pacific Privacy Authorities (APPA) forum in Macau (December 2015).

Royal Commission into Family Violence

Information sharing also featured as a prominent theme in the Victorian Royal Commission into Family Violence (RCFV). Following a written submission to the RCFV, the Commissioner produced a witness statement and gave oral evidence to the RCFV at one of the two hearing days dedicated to integrating services and information sharing. The issues raised by the Commissioner in his evidence included:

- the barriers to information sharing, which prevent organisations from sharing information, even where they have the legal authority to do so
- misconceptions of privacy law, which lead organisations to believe they are unable to share information with other organisations
- how the public sector can improve its information sharing practices to address family violence, in a way that is consistent with privacy legislation
- the need for an information sharing culture to emerge, which requires sound governance and leadership at an executive level.

The RCFV final report was tabled in the Victorian Parliament in March 2016. It included 227 recommendations for improving all aspects of the family violence system, with five directly related to information sharing. These recommendations indicate that CPDP will have a significant role to play in guiding their implementation by the Victorian Government. In particular, recommendation 6 proposes CPDP involvement in a working group to promote an information sharing culture.

New technology

Cloud computing

Following the publication of a discussion paper on cloud computing in the previous reporting period, CPDP held a public forum on cloud computing in July 2015. The forum was attended by both public and private sector representatives, and explored issues including the risks associated with cloud computing, building in privacy and security measures upfront, risk management throughout the information lifecycle, and how cloud computing fits into the broader narrative of public sector outsourcing arrangements.

Big data

Big data has continued to be a major research focus for CPDP, and the Commissioner has commenced two collaborative partnerships in the big data space. The first is with Deakin University in its work with the Data to Decisions Cooperative Research Centre (CRC). The CRC brings researchers and industry together to develop a big data capability for national security purposes and a sustainable big data workforce. This is an important piece of work given that big data analytics has become a mainstream approach to interrogating data in the private sector, and is gaining traction within government. Through Deakin University, CPDP will contribute to the research and analysis being undertaken by the CRC in the law and policy project – one of several parallel projects – which explores the development of a new regulatory regime for big data.

The second collaboration is with the United Nations Special Rapporteur on the Right to Privacy (SRP). The SRP's mandate covers six key themes, one of which is big data and open data. The Commissioner has been appointed the world lead on the work being undertaken internationally on the big data and open data stream, and will assist the SRP to coordinate the work and manage the global team of researchers. Some of the areas of inquiry that the project will focus on include defining big data, the technologies involved in performing advanced data analytics, the legal and regulatory considerations, and how we might address the various risks that big data and open data pose to privacy. CPDP will contribute to planning the project and conducting research, the end result of which will be a report presented to the United Nations General Assembly. The end product of this major piece of work will inform the guidance that CPDP provides back to the Victorian public sector on how to manage and minimise the risks involved in engaging with big data and open data.

De-identification

CPDP has commenced work on de-identification, looking at the merits and challenges with using it as a privacy-enhancing technique. As part of PDP Week 2016 CPDP held a public forum on de-identification and invited notable experts to speak to this topic. The forum was well attended by members of the public sector and the general public. A background paper was also produced to inform discussion at the forum, which was published to the CPDP website. The learnings from the forum will contribute to future work in this area.

Smart cities

The smart cities concept is gaining momentum in cities all around the world, including Melbourne and other Australian cities. A 'smart city' is one that uses technology to enhance the way it delivers services, manages resources and generates growth opportunities to promote efficiency, affordability and sustainability in urban areas. Smart cities operate through the integration of technology with infrastructure, employing a data-driven approach to urban design, planning and service delivery. This is facilitated through data analysis, sensor technologies and urban experiments.

Recognising that there is the potential for privacy and security concerns to stem from smart cities and other Internet of Things technologies, CPDP held a second expert forum during PDP Week 2016 on smart cities, and also produced a background paper on this topic. CPDP will continue to monitor developments in the smart cities space, and work with state and local governments on their future projects.

Biometrics

CPDP has been an active participant in the biometrics space, and has consulted with a number of organisations – both at state and national levels – on various projects that use biometrics for identity management purposes. CPDP undertook a piece of work to update a 2012 guidance document that the former Office of the Victorian Privacy Commissioner produced, taking into account developments in technology and privacy expectations in the biometrics space since then.

CPDP is represented on the Biometrics Institute Privacy and Policy Experts Group, and the Commissioner hosted a Biometrics Institute member meeting in Melbourne in June 2016.

Tools and resources

In March 2016 CPDP launched its *Introduction to privacy in the Victorian public sector* online training course. The training provides public sector staff with an overview of their privacy obligations under the *Privacy and Data Protection Act 2014* and contains a series of interactive questions to test individuals' knowledge. In addition to the online course, CPDP produced a downloadable version of the training that can be presented to groups for in-house training. The online course has had significant up take and CPDP has received positive feedback on its content.

As part of an ongoing project to update guidance material published by the former Office of the Victorian Privacy Commissioner, CPDP has produced a number of new information sheets for use by public sector organisations, which includes an information sheet on the various pieces of privacy legislation in Victoria, and another on how to manage privacy in emergency situations. As CPDP does not have the capacity to produce resources on all matters of interest, the office has produced an annotated link library on the CPDP website that links to authoritative guidance and informational documents that have been published by others. The link library will be updated periodically as new resources become available.

CPDP has also launched a Twitter account (@CPDPVICAU), which is used to promote new publications, events and interesting news items related to privacy and data protection. It has proved a useful tool for engagement with stakeholders and for keeping informed about the work of other privacy and data protection regulators.

Flexibility mechanisms

In March 2016 the Commissioner certified the first information usage arrangement (IUA) under the *Privacy and Data Protection Act 2014*. The IUA was made in respect of Risk Assessment and Management Panels (RAMPs), which sought to depart from five of the IPP provisions as well as information handling provisions in other acts, to facilitate the ability of specified parties to work together to respond to family violence. The Commissioner certified that there was a substantial public interest in permitting departures from the relevant provisions for RAMPs purposes.

The experience of working through the first IUA application required CPDP to develop its own internal processes regarding the format an application should take, what supporting documentation should be submitted to the Commissioner (such as a PIA), timeframes, and the ongoing relationship between CPDP and the lead party to the IUA. The experiences of the RAMPs IUA will inform the Commissioner's approach to assessing future applications for flexibility mechanisms.

In addition, the Commissioner has received three other requests for pre-application consultations, and a number of general enquiries about the flexibility mechanisms. One application for certification had been received during this time, but was not finalised by 30 June 2016.



Data Protection

The key role of the Data Protection Branch of CPDP has been the development of the Victoria Protective Data Security Framework (VPDSF), the Victorian Protective Data Security Standards (VPDSS), which sit at the heart of the Framework, and an Assurance Model to monitor their uptake and implementation by the Victorian public sector.

Given the vast volume of sensitive and significant (valuable) information processed or held by Victorian public sector organisations, secure management of information, assets and services is critical to Government service delivery, public safety and citizens' way of life. By implementing protective security measures, Government can guard information against a range of threats.

Valuing Public Sector Data

CPDP is working with government to emphasise the importance of understanding information assets held by the Victorian public sector.

In order to help Victorian public sector organisations to assess the value of the information they use everyday CPDP developed a mobile and desktop application. This application not only assists with undertaking a timely and holistic assessment of official information but also enhances end user awareness of the valuation process and the protective markings used in Victorian government.

Given the popularity and take up of mobile apps, combined with bespoke functionality that can be built into these, CPDP developed the automated Business Impact Level (BIL) assessment app reflecting the BIL table used in the VPDSF.

This app takes similar apps used elsewhere e.g. NSW government classification and labelling app (<https://www.finance.nsw.gov.au/ict/app/>) one step further by stepping end users through the valuation assessment process of not only the confidentiality of the information but also the integrity and availability attributes to identify:

- the appropriate protective marking / security classification for the information
- any enhanced security controls designed to further protect the material

The development and roll out of a BIL assessment app is expected to provide benefits, including:

- promote compliance with the VPDSS
- deliver public value by enabling efficient and effective use of resources within the Victorian public sector
- establish a proper understanding for a holistic assessment of official information, beyond that traditionally set out under the Australian Government Protective Security Policy Framework (i.e. encompassing confidentiality, integrity and availability)
- engagement of Agency Heads / Executives in the assessment process, as it is readily accessible and can be downloaded onto Apple and Android mobile operating platforms

- assist CPDP to engage with a broad user base both across the VPS and interested Contracted Service Providers (CSPs)
- potential to assist users in conducting a threat assessment to determine whether a 'serious' threat threshold has been met

The BIL assessment app has been met with positive feedback. CPDP consulted with and piloted the app with a number of stakeholders both local and national who have been impressed by its usability and accessibility. Given its adaptability, interstate stakeholders have also shown an interest in adopting the app and modifying to suit their local context. With the VPDSF table now finalised and published, the app is in its final stages of development and will be published as a VPDSF resource to use in the coming period.

What is the Victorian Protective Data Security Framework?

The Victorian Protective Data Security Framework (VPDSF) is the overall scheme for managing protective data security risks in Victoria's public sector. Established under Part Four of the Privacy and Data Protection Act 2014 (PDPA), the framework consists of the:

- Victorian Protective Data Security Standards (VPDSS)
- Assurance Model
- supplementary security guides and supporting resources.

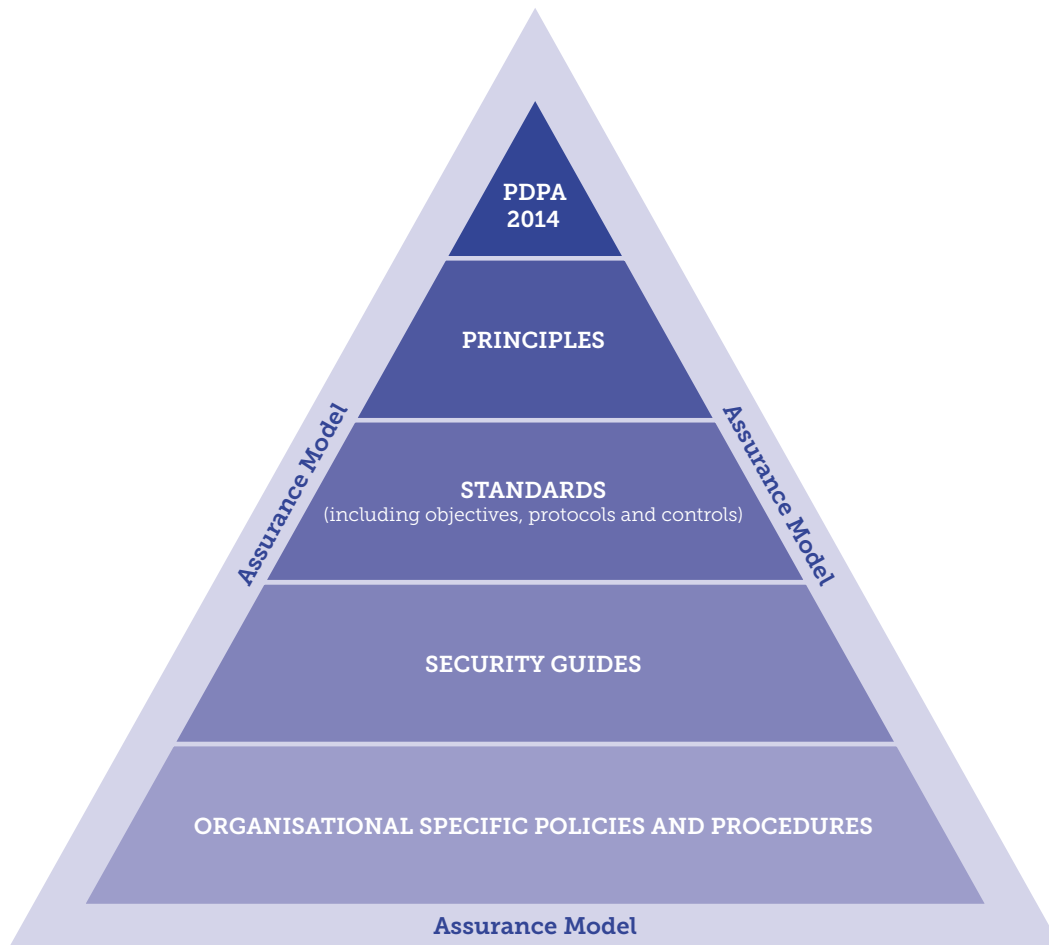
The VPDSS assist government operations by ensuring the right people have access to the right information at the right time. Based on national and international protective security policies and practices, the standards align with security measures established in the Australian Government Protective Security Policy Framework (PSPF). They also recognise the Victorian public sector's unique operating requirements and diverse range of agencies and bodies.

The Assurance Model sets out monitoring and assurance activities that assist public sector organisations to comply with Part 4 of the legislative requirements of the *Privacy and Data Protection Act 2014* with regard to data security. The ultimate aim of the Framework and its Standards is to ensure the public has confidence in the public sector's protective data security practices. The Assurance Model also enables the Victorian Government to monitor and measure the security capability, resilience, efficiency, effectiveness and economic benefit of these practices.

Most importantly, the VPDSF encourages cultural change in the Victorian public sector by promoting protective data security as part of everyday business. Public sector organisations will then manage security risk more effectively and contribute to innovation and increased productivity, while maintaining a secure government operating environment.

CPDP will continue to develop and refine the protective data security framework with the Victorian public sector to achieve the most efficient, effective and economic delivery of Victorian Government business

A visualisation of the VPDSF is as follows:



The principles

The Victorian Protective Data Security Framework and its Standards are principle-based. The guiding principles were developed to enable organisations to evaluate their current and prospective security practices:

1. strong governance arrangements ensure the protective data security business requirements are reflected in organisational planning
2. risk management empowers an organisation to make informed decisions and prioritise security efforts
3. understanding information value informs an organisation's application of security measures to protect information
4. a positive security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services
5. a continuous improvement lifecycle model enables an organisation to systematically identify opportunities to mature its protective data security practices
6. sound protective data security practices assist an organisation to achieve its objectives in an efficient, effective and economic manner.

The standards

By the end of the reporting period, the Victorian Protective Data Security Standards (VPDSS) had been developed, following wide stakeholder consultation and were awaiting Ministerial approval before being issued.

The Standards establish 18 high level, mandatory requirements to protect public sector data and provide for governance across the four protective security domains: Information security, Personnel security, ICT security and Physical security.

Each standard is supported by four protocols. This follows the continuous improvement process of 'plan, do, check, and act', enabling organisations to continually assess their security controls against any new or updated threats and vulnerabilities.

The standards:

- take into account the policy and operational responsibilities of the Victorian Government
- respect the important role that Victorian public sector organisations play in delivering critical services
- reflect national and international approaches to security, but are tailored to the Victorian environment
- focus on the security of information held by the Victorian public sector, rather than all official assets
- identify information security and ICT security as individual yet equally important security domains
- require contracted service providers with direct or indirect access to information to adhere to the standards.

The standards are durable and take a risk management approach that empowers government business to function effectively, safely and securely.

The assurance model

The Assurance Model enables organisations to measure the maturity of its implementation of the VPDSS.

The model aims to:

- enhance the maturity of your organisation's protective data security practices
- provide assurance to government of the security of information.

The model is unique in placing the focus on the identification of information, information assets and information systems, intelligence driven threats, vulnerabilities and detailed real world security risks. The result will be a more informed selection and investment in security controls commensurate with the value of the information.

The security risk management and control selection will prepare organisations to complete the annual compliance self-assessment and security capability maturity assessment. All of this will be captured in the monitoring and assurance system to provide two valuable outputs,

- ministerial reporting to assure the Victorian Government that organisations are adopting the VPDSS and in turn securing Victorian public sector data
- conduct research and analysis to provide security practitioners with actionable protective data security intelligence.

Resources

CPDP has produced and will be producing a significant amount of material to assist public sector organisations lift their current information security capability and maturity. Current published guidelines include:

- *Victorian Protective Data Security Framework*
- *Draft Victorian Protective Data Security Standards* (visual representation)
- *Assurance Model* (visual representation)
- *Glossary of Protective Data Security Terms*
- *Rosetta Stone* to assist with mapping existing security frameworks to the VPDSF
- *Data Protection and You - What you need to know*. A video for the Victorian public sector
- *Information Security Guide*. This guide includes:
 - Chapter 1 – Understanding Information Value
 - Chapter 2 – Protective Markings
- CPDP Application
- Video.



Law Enforcement Data Security

Part 5 of the *Privacy and Data Protection Act 2014* calls out law enforcement data security as a special case within the framework of protective data security and extends the Commissioner's jurisdiction to cover both Victoria Police and the Victorian Crime Statistics Agency.

Crime Statistics Agency

The Crime Statistics Agency was established in 2014. It is an agency independent of Victoria Police with responsibility for producing Victoria's official recorded crime statistics, and conducting research into crime and criminal justice trends.

The nature of the work undertaken by CSA entails it receiving and holding law enforcement data.

Under s.92(1) of the *Privacy and Data Protection Act*, the Commissioner has developed and issued the *Crime Statistics Data Security Standards* (CSDSS). With the interim standards being issued in March 2015, CSA conducted a compliance gap analysis against them in June 2015 that formed the basis of their obligations for annual assurance reporting to CPDP.

In accordance with the Governance requirements set out in the CSDSS, the CSA has conducted assurance reporting for 2015-16. The CSA has provided assurance to the Commissioner for Privacy and Data Protection that there is a Security Management Framework in place consistent with the requirements set out in the CSDSS. Furthermore, CSA have provided assurance that security controls in place to mitigate identified risks to crime statistics data of the Crime Statistics Agency are adequate.

Victoria Police

Implementation of Recommendations

Implementation Working Group (IWG)

The joint Victoria Police and CPDP IWG continued to meet and progress outstanding recommendations throughout 2015-16.

A core component of the IWG is the continued focus on relevant, accurate and timely communication between Victoria Police and CPDP. The IWG has worked hard to develop a clear picture of outstanding recommendations, including the capacity to implement outstanding recommendations moving forward.

Victoria Police has implemented six recommendations in 2015-16 and has delivered a further 14 recommendation responses for consideration in meeting implementation.¹ This is a significant achievement given that most outstanding recommendations are IT/System specific and often require business case funding.

1 These responses were delivered after the financial year deadline but should still be considered as work undertaken within 2015-16. The outcome of these responses will be reported in the Annual Report 2016-17.

New Assessment Category

In December 2015, CPDP issued a new assessment category *Not Implemented – Risk Managed*. This category supports existing categories of *Implemented*, *Not Fully Implemented* (partially implemented), and *Not Implemented*.

This assessment category can be issued in cases where Victoria Police have a justified lack of capability and/or intent to implement a recommendation within a reasonable timeframe. If issued, the category recognises that Victoria Police has initiated and applied appropriate risk management and governance controls. Any risk/s associated with not implementing a recommendation sit wholly with Victoria Police.

While any assessment of *Not Implemented – Risk Managed* finalises an outstanding recommendation, CPDP may conduct future reviews or audits on Victoria Police that raise or address similar or related issues. Any future recommendations will be reviewed on their own merits.

In 2015-16, no outstanding recommendations were finalised as *Not implemented – Risk Managed*.

Breach Reporting – Security Incident Register

In 2013 Victoria Police initiated the Security Incident Registry (SIR) as the central organisational repository for the reporting, recording, recovery and post-incident analysis of information security incidents and events. The register is important in that it is designed to capture security incidents or events that do not necessarily involve misconduct or criminal activity.

It does however record and maintain all information security incidents reported to and by the Professional Standards Command (PSC).

Status	Pre IWG	30/6/12	30/6/13	30/6/14	30/6/15	30/6/16
Implemented	41	71	132	164	166	172
Not Fully Implemented	110	54	41	25	24	24
Not Implemented	62	56	41	23	30	24
Withdrawn	0	32	39	41	41	41
Total Recommendations	213	213	253	253	261	261
Total Outstanding	172	110	82	48	54	48
% of active recommendations implemented	19%	39%	62%	77%	75%	78%

Implementation of recommendations

SIR statistics

CPDP receives weekly reports from the SIR that include all incidents captured over the preceding week. The weekly report also provides 'notable developments' to reported incidents including new information, changes to impact assessment or status progress.

The SIR also reports incidents on a case-by-case basis to CPDP under the escalated reporting protocol.

The SIR designates each information security incident a security domain, or domains, as applicable (Information, ICT, Personnel or Physical) and assesses and records the incident against a pertinent typology. The SIR conducts an initial, and ongoing, assessment of the potential or actual consequence of each incident and engages relevant subject matter experts to provide organisational oversight, remediation, and ongoing reviews as required.

In 2014-15, the SIR recorded 332 information security incidents. In 2015/16 the SIR dealt with 453 information security incidents – a 36% increase from the previous financial year. This increase is almost certainly driven by improved organisational maturity around information security incident identification and reporting, and enhanced information capture by the SIR.

At 30 June 2016, 385 incidents were marked complete, with 21 being found to constitute no information security incident upon file completion. 68 incidents remain in progress (including those reported to the SIR by PSC - see the 'PSC reporting to the SIR' section for further discussion).

Figure 1. Security incidents reported by month 2015-16

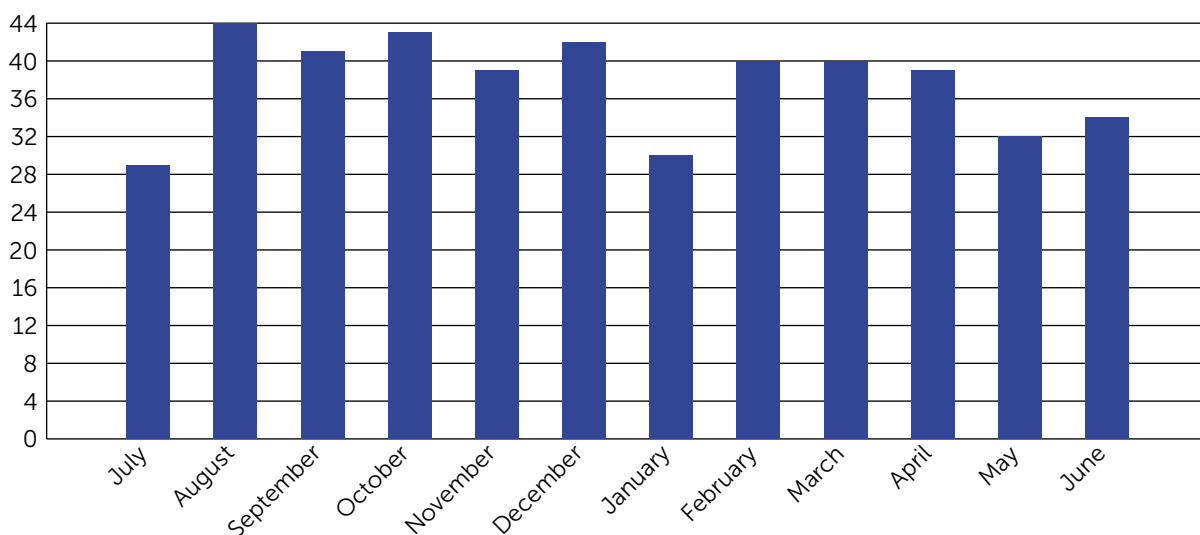


Figure 2. Information Security Incidents – By Major Type

Type	Count
Lost or Stolen Police Certificates of Identity	207
Unauthorised Release or Disclosure of Information	40
Data Spill (including exposure to police information)	32
Unauthorised Access	27
Theft or Loss of Asset	21
Malware Infection	19
Abuse of Privilege	18
Failure of Process	10
Threat to Facility	9
Unprofessional Conduct	9
Access Controls	5
Denial of Service	5
Other Event	5
Password Confidentiality	5
Stolen Victoria Police Credentials	5
Unauthorised Changes to Information, Applications, Systems or Hardware	5
Configuration Error	4
Fraudulent Activity	3
Damage to Asset	1
Social Engineering	1
Suspicious System Behaviour or Failure	1

Figure 3. Potential or actual consequence assessment (as at 30 June 2016)

Incident Assessment	Count
MAJOR	1
MODERATE	20
MINOR	83
INSIGNIFICANT	291
No Incident	21
Unable to assess	37

Escalated Reporting Protocol

The Escalated Reporting Protocol was designed in consultation with Victoria Police to set out operational requirements and processes relating to the Commissioner's access to Victoria Police security incident information.

Having regard to the intent of standard 32 (*Standards for Law Enforcement Data Security, or SLEDs*), the protocol's purpose is to establish mechanisms and rules that:

- determine security incident assessment levels against potential or actual consequences
- support timeframes for reporting security incidents to the Commissioner for Privacy and Data Protection
- provide the methods to report a security incident to the Commissioner for Privacy and Data Protection.

The Protocol establishes expectations that security incident reports received from the SIR provides a holistic assessment of the incident including, but not limited to:

- the context of the incident occurring
- characteristics of the incident
- affected workgroup/s (including the information owner, information custodian and any external parties or stakeholders)
- timelines around the incident occurring (including identification, reporting etc.)
- breadth of exposure
- potential or actual consequences
- impact upon individuals, work unit or the organisation including service delivery

As at 30 June 2016, 100 information security incidents had been reported to CPDP under the obligations set out in the escalated reporting protocol. This protocol is an important facet of CPDP's monitoring and assurance activities and is designed to provide the Commissioner with relevant, accurate and timely advice on significant and sensitive information security incidents impacting law enforcement data.

Breach Reporting – Register of Complaints, Serious Incidents and Discipline (ROCSID)

ROCSID is a database used by Professional Standards Command (PSC) to record, manage, and investigate incidents that amount to corrupt behaviour, criminality or misconduct, including breaches of information security.

This year, CPDP has undertaken the monitoring and reporting of ROCSID data differently. Change was made to deliver more relevant, accurate and timely analysis to the Commissioner on allegations of information security breaches involving misconduct, corruption or criminality. ROCSID files were individually reviewed on a quarterly basis, and findings reported the Commissioner. These quarterly reports outline the *context* of breaches, and are an important internal briefing tool in the Commissioner's monitoring and assurance activities under the *Privacy and Data Protection Act 2014*.

ROCSID Statistics

While reporting methodology has changed from 2014-15, the basis of interrogating the ROCSID database remains standard. CPDP extracted data via a standardised report function executed within the ROCSID database.

The report returned 211 incidents containing an information security element recorded in ROCSID in 2015-16.²

This number is substantially lower than the 348 incidents recorded in 2014-15. This discrepancy is the result of LEAP audit files no longer being recorded by PSC on the ROCSID database.

42 ROCSID files confirm an information security breach, or breaches, while 45 files are still under investigation.

PSC reporting to the SIR

As noted, the SIR is the central register of all security incidents including PSC investigations involving breaches of information security. The SIR has access to, and oversight of, relevant PSC investigations reported to, or by, the SIR.

For 2015-16 the SIR recorded 81 information security incidents reported to them by PSC. As at 30 June 2016, 44 investigations had been reported by PSC as being completed, with 37 incidents still under investigation.

Issues with SIR and ROCSID data correlation

ROCSID data is liable to change as files are subject to reclassification at any stage – often information security breaches are only identified in the course of an investigation spanning weeks or months. At any stage, files may be in, or out of, scope as investigations mature and develop a more complete picture of the incident. As such reporting to the SIR can be adversely affected.

While the SIR undertake monitoring activities of the ROCSID database as part of their information collection priorities, the recording of ROCSID breaches onto the SIR register is dependent on an assessment against internal SIR criteria. While it is likely that this process captures a significant proportion of both serious or overt information security incidents, for CPDP there remains a serious inability to interrogate SIR reports against ROCSID data, and vice versa.

2 Report generated 8 August 2016. Figures are correct at time of compilation. Factors such as re-classification of files, and ongoing quality control by Victoria Police, will cause variations in extracted data.

Review of Victoria Police Security Incident Management framework and practices

In May 2016, CPDP engaged KPMG to conduct a review into the Security Incident Management framework and practices of Victoria Police.

The review aims to determine the extent to which Victoria Police has implemented an effective Security Incident Management (SIM) framework, and practices. The Office of the Commissioner for Privacy and Data Protection's (CPDP) objectives for an effective SIM framework for Victoria Police are:

- to allow timely and corrective action to be taken in the event of an information security incident in order to protect law enforcement data and reduce the impact and likelihood of damage caused by a failure of information security controls.
- to ensure feedback on incidents and that information security incident management procedures can be continually improved so that future incidents are better managed.

These requirements are documented in the *Standards for Law Enforcement Data Security 2014*, specifically under Standards 32 and 33. These Standards are enacted within the *Privacy and Data Protection Act 2014*.

The review is expected to cover:

- 1) the identification of best practice Security Incident Management (SIM) and validation of CPDP Incident Management Framework (IMF).
- 2) the critical assessment of the overarching Victoria Police Security Event / Incident Management Framework and practices covering:
 - a. all security domains including physical, personnel, information and ICT
 - b. relevant organisational policies and guidelines
 - c. governing legislation and standards, specifically Standards for Law Enforcement Data Security (SLEDS), Australian Government Protective Security Policy Framework (PSPF), and Australian Government Information Security Manual (ISM).
 - d. organisational governance and strategic direction
 - e. security incident subject matter expertise / portfolio holders
 - f. current security incident lifecycle practices (preparation, detection, handling, prevention)

- 3) a gap analysis between best practice security incident management and current Victoria Police framework and practices.
- 4) the development of recommendations to optimise and innovate whole-of-Victoria Police response to current issues and emerging trends in security incident management.

Importantly the review will assist in validating a draft CPDP Incident Management Framework against best practice.

Findings from the review are currently being assessed and developed into recommendations. Working closely with Victoria Police, the report is expected to be finalised and delivered in the first few months of the 2016-17 reporting period.

Site Inspections

Under the *Privacy and Data Protection Act 2014* CPDP is authorised to conduct monitoring and assurance activities, including audits, to ascertain Victoria Police compliance with the law enforcement data security standards. These activities include, but are not limited to, conducting site inspections of Victoria Police facilities.

The site inspections are designed to interrogate themes relevant to the facility, and consider organisation issues that play out at the local level 'on the ground' in operational policing environments.

The 2015-16 site inspections maintained the style and scope undertaken in 2014-15 following a theme-based enquiry. This allowed CPDP to consider key information security priorities being focused on by both Victoria Police and CPDP at an operational and strategic level. The site inspections considered themes including the lifecycle management of law enforcement data, information security incident response, management and reporting, the use of mobile devices, and information sharing. Interviews were conducted with a broad range of VPS and sworn staff across work units to focus on members' knowledge or and response to these themes.

Three site inspections were undertaken being Mansfield Police Station in October 2015, the Morwell Police Complex in January 2016, and the Dandenong Police Complex in May 2016.

There were various stand-out findings from these site inspections.

Sworn staff continue to remain confused or unaware of organisation policy around information classification and the use of protective markings. There also remains a cultural divide between sworn and VPS staff in understanding the 'value' of law enforcement data handled in their respective roles – with VPS staff often believing their role was 'administrative' even when handling the same law enforcement data as their sworn counterparts.

The breadth and depth of exposure to law enforcement data by VPS staff is substantial and significant, and VPS staff continue to have limited or no awareness of organisational measures around information security. VPS staff further indicated that they received no training in information security.

All Victoria Police employees continue to rely heavily on hardcopy law enforcement data. This requirement is being driven and exacerbated by operational necessity, including the duplication of effort required to input information into multiple systems that often do not integrate. Sworn officers, in particular, continue to maintain the unofficial storage of significant volumes of hard and electronic law enforcement data – under desks, in correspondence lockers, or in personal equipment lockers.

Digital asset management (electronic law enforcement data) is now imbedded as a key component of the modern policing environment. Overall, the management of digital assets was inconsistent, and often incorrect. There is a lack of knowledge around the approved use of Victoria Police ICT systems to store and manage digital assets for investigation and intelligence purposes.

In this respect, personal computing devices are continuing to be used for work purposes – the capture, storage, and sometimes transmission, of law enforcement data. Often law enforcement data was not deleted from personal device storage, and therefore devices often carried data from multiple incidents, work locations, or day-to-day activities.

Sworn and VPS staff reported that confusion around work expectations, including a focus on information security, was being driven by the depth and breadth of requirements placed upon them to undertake their duties. Documentation that supported local and organisational information security was considered by staff as either too complicated, or not easily found.

Local documentation was often not available, not complete or in draft format, out-of-date, or did not include any specific reference to information security.

Survey of Victoria Police Members

CPDP and Victoria Police completed the third, and final, wave of a quantitative longitudinal survey examining the information security culture amongst sworn Victoria Police members. Conducted in March and April 2016, the survey complements and extends findings from the 2014 survey, and the benchmark data obtained in 2012.

The longitudinal survey was designed to provide key indications of the efficacy of the Victoria Police cultural change program, specifically to examine the effectiveness of information management and information security initiatives around training and awareness.

The response rate to wave 3 was 16% of the sworn workforce, delivering a robust statistical sample. To further enhance and define analysis, results were weighted to align more closely with the relevant Victoria Police census of sworn staff.

Key high-level findings from the 2016 survey were that:

- knowledge as to what constitutes 'law enforcement data' is not well established
- a substantial minority of sworn members would 'work around' an issue to get the job done rather than adhere to restrictive policy and procedure
- member highlighted concern around lack of adequate storage space driving personal holdings of law enforcement data; and a high perceived likelihood that third party contractors would be unsupervised on station premises
- members highlighted three broad areas of data security breach risk (by likelihood) including:
 - the use of personally owned electronic equipment to capture and store law enforcement data
 - requirements to operate out of unsecured offices
 - the electronic transfer of law enforcement data, particularly through the use of USBs
- the highest incidence of personally owned (and used) technology centred on mobile phones, USBs, and portable audio/visual recording devices

Longitudinal developments 2012 - 2016

In the 2016 survey, awareness of changes to information management and information security requirements (both organisationally and locally) was substantially lower than recorded in 2014. This suggests that, for many sworn members, information management and security changes are becoming increasingly embedded in daily processes as 'business as usual'.

Other high level longitudinal findings highlighted between 2012 and 2016 around attitude and behaviours include:

- an increasing reference by sworn members to standards and manuals as the primary source of guidance around information management and security.
- that any (unintentional) breach via the electronic transfer of files (particularly through the use of USBs) is seen as less serious than in previous years. This is likely due to the contemporary policing operating environment increasingly relying on complex digital asset management to undertake their law enforcement functions.
- an increase in the likelihood of use of personal electronic equipment (such as 'smart' mobile phones) to capture and store law enforcement data in the course of duties.
- that personal holding of law enforcement data continues to have a high likelihood of occurrence driven by limited storage space, a continued reliance on hardcopy as well as electronic data, and the belief in the need to capture personal records of work activities.

A full report drawing together the longitudinal survey results, site inspection findings, and analysis of the Victoria Police cultural change program is currently being undertaken for delivery in 2016-17.

Cultural Change

In reviews conducted in 2009 and 2011, the Commissioner recommended that Victoria Police develop and implement a plan for information security cultural change.

Victoria Police continued cultural change implementation activities throughout 2015-16, notably:

- initiating the roll-out of Information Management & Information Security (IM&IS) portfolio holders across relevant stations, work units, divisions and departments
- the establishment of an online information security learning module
- the implementation of a Facilities Security Risk Assessment. This document develops a consistent mechanism to assess physical security risks and identifies mitigation strategies and is supported by a strict compliance regime.
- the establishment of an amnesty for personal holdings of law enforcement data encouraging employees to declare and bring in all holdings for destruction or archiving.
- the development of a measurement tool and process to be used to assess the level of information management maturity within Victoria Police. This tool is to be used on an ongoing basis to identify areas to be addressed.

Policing Information Process and Practice (PIPP) reform project

The PIPP project was launched in 2013 to provide members with the capability to securely access information where and when they need it.

Significantly re-imaged and re-focussed in 2016, the project is now titled the *BlueConnect* program and includes three technology-enabled programs being:

1. mobile technology – delivering handheld mobile devices to frontline police
2. intelligence capability – a new system to provide Victoria Police with enhanced intelligence analytics
3. case management – the conduct of a proof of concept activity to determine the future case management solution for policing

The *BlueConnect* project team recognise that security will be an important part of organisational change management (including training, awareness, policy and processes). The project will encompass and deliver strong IT controls framework around ICT systems that will improve data quality over time and ensure data security.



Privacy and Data Protection Networks

The Office of the Commissioner for Privacy and Data Protection conducts a very broad and full program of consultations across the Victorian public and private sectors, academia and national and international bodies.

Importantly, CPDP conducts a number of forums and events and participates actively in others.

Youth Advisory Group

Children and young people represent an important stakeholder group for CPDP, as potentially the most vulnerable to the misuse of their personal information or improper data handling. To mitigate potential risks, it is important that children and young people be educated about the importance of privacy and data protection, and given the tools and skills they need to protect themselves and their personal information.


CPDP's Youth Advisory Group (YAG), re-established in early 2015, provides the Office with a means by which it can identify and address the specific privacy and data protection needs of children and young people through means such as Whole of Victorian Government policy development and communications. During the reporting period, members of the group participated in the 2016 Global Enforcement Network (GPEN) privacy sweep and conducted the public forum *'Privacy: Who cares?'* during May's Privacy and Data Protection Week.

Inter-agency Privacy Officers' Forum

The Inter-agency Privacy Officers' Forum was established in 2015 to facilitate ongoing dialog in relation to operational and policy-based privacy and related issues. Membership of the group consists of staff from CPDP, in particular from the Operational Privacy and Assurance and Strategic Privacy Branches, as well as Privacy Officers and/or staff with privacy responsibilities from the seven central departments, and key agencies including Victoria Police, VicRoads, WorkSafe Victoria and Public Transport Victoria. Meetings are held quarterly.

Privacy and Data Protection Week

Each year in May CPDP participates in Privacy Awareness Week, an initiative of the Asia Pacific Privacy Authorities (APPA). This year, CPDP rebranded the week as 'Privacy and Data Protection Week' in order to include the office's data protection responsibilities. During Privacy and Data Protection Week CPDP held a number of events, including a PDP Week launch, two public forums, information sessions conducted jointly with the Office of the Freedom of Information Commissioner and the Health Services Commissioner, information sharing training sessions, and a Youth Advisory Group



forum. Importantly and for the first time, CPDP widened the scope of the week to include major Victorian regional centres.

Privacy Authorities Australia

The Commissioner is a member of the Privacy Authorities Australia (PAA) forum, which is made up of privacy regulators from each Australian state, territory and the Commonwealth. In January 2016 the Commissioner hosted a PAA meeting in Melbourne. At this meeting the Commissioner screened a pre-recorded interview with the United Nations Special Rapporteur on Privacy, who spoke about the challenges facing privacy regulators around the world. The Commissioner and Assistant Commissioner for Strategic Privacy also attended a subsequent PAA meeting in Sydney.

Asia Pacific Privacy Authorities

The Asia Pacific Privacy Authorities (APPA) is the principal forum for privacy authorities in the Asia Pacific region to come together to exchange ideas and learn from each other's experiences. The Assistant Commissioner for Strategic Privacy attended the 44th meeting of APPA in Macau in December 2015, presenting a paper on work done by CPDP on information sharing. Topics discussed at the meeting included data breach notifications, the Safe Harbour framework and big data. CPDP has also been an active participant in responding to consultations and surveys run by the APPA secretariat.

Global Privacy Enforcement Network

CPDP is an active member of the Global Privacy Enforcement Network (GPEN), which is an informal network of privacy and data protection authorities from around the globe that work to foster cross-border cooperation. In 2016 CPDP participated in the annual GPEN Sweep, the theme of which was 'Internet of Things with a focus on accountability'. CPDP examined the privacy policies of local councils to determine whether or not local councils adequately communicate to individuals about their privacy practices in relation to CCTV.

CPDP also regularly participates in GPEN conference calls with other members and is on the GPEN Pacific Program Committee, which assists to identify topics and speakers for conference calls.

UN Global Pulse

The Commissioner has continued his role as a member of the UN Global Pulse Data Privacy Advisory Group, and regularly participates in UN Global Pulse teleconferences and contributes to their work program.

All-States Data Security Group

As part of stakeholder engagement and keeping abreast of security programs underway across Australian and State governments, CPDP hosted in October 2015 one of the bi-annual scheduled meetings of State and Territories security representatives. Attendees included representatives from the Queensland Government CIO, Public Safety Business Agency, Transport NSW, the Office of the Digital Government South Australia, the Tasmanian Department of Premier and Cabinet, and representatives from the Governments of Victoria, ACT and Northern Territory and the Commonwealth (Attorney-Generals Department and the Department of Prime Minister and Cabinet).

The meeting covered local issues and current security programs of work, discussions around monitoring and assurance activities, protective markings used across the States and Territories, roles and responsibilities (RACI model) of primary points of contact for each protective security domain for each State/territory, Commonwealth briefing on Protective Security Policy Framework updates and the cyber security strategy development.

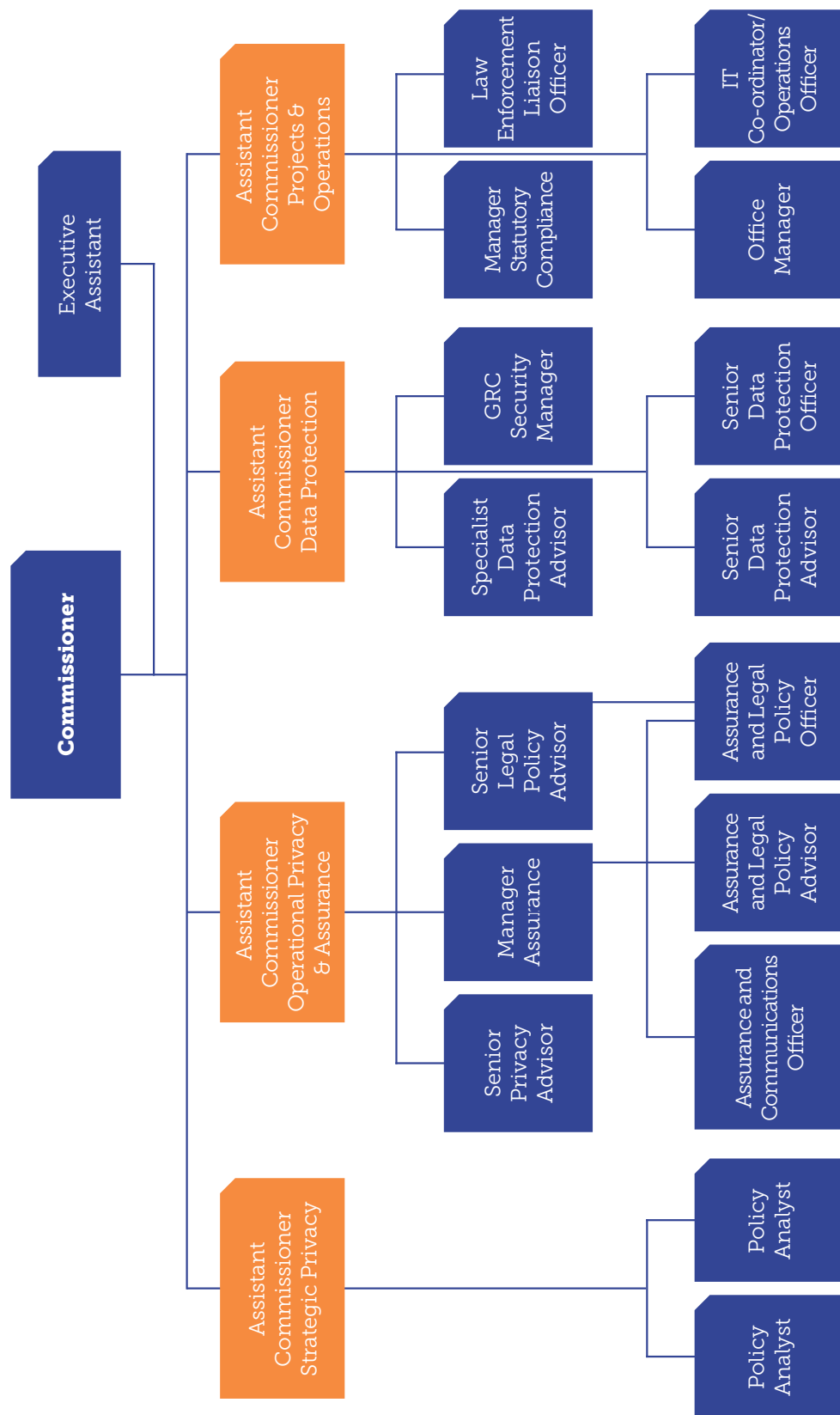
The discussions between stakeholders continued at the following bi-annual State and Territories security representatives meeting in May 2016 in Queensland where representatives from CPDP attended and topics including security governance structures, breach notification, incident response, information sharing, vulnerability scanning activities and maintenance of policies were discussed.



About the Office of the Commissioner for Privacy and Data Protection

The Office of the Commissioner for Privacy and Data Protection was created as a statutory agency by the Privacy and Data Protection Act 2014 and came into existence on 17 September 2014.

Organisational Structure and Staffing



The Office of the Privacy and Data Protection also includes an Audit and Finance Committee comprised of three external members, governed by a Charter.

The Office had a staff of 21.8 FTE at 30 June 2016, of which 1FTE was on secondment to the Department of Justice and Regulation, 3.4FTE on fixed term contracts and 17.4 FTE on-going members of the Victorian Public Service.

Gender	On-going	Fixed term	Secondment
Female	9	1	1
Male	8.4	2.4	0

Age	On-going	Fixed term	Secondment
Under 25	1	0	0
25 – 34	5	0	1
35 – 44	5	1	0
45 – 54	3	1	0
55 – 64	1.8	1.4	0
Over 64	1.6	0	0

Classification	On-going	Fixed term	Secondment
VPS2	0	0	0
VPS3	2	0	1
VPS4	4.4	1	0
VPS5	5.6	0.4	0
VPS6	4.6	1	0
STS	0.8	0	0
Statutory Office Holder	0	1	0

The Commissioner is committed to applying merit and equity principles when appointing staff. The selection process ensures that applicants are assessed and evaluated fairly and equitably on the basis of key selection criteria and other accountabilities without discrimination. The Commissioner offers a flexible working environment and is committed to fostering diversity in the workplace.

Governance and Reporting

CPDP maintains a compliance register that includes its statutory obligations.

Regular reports track progress in achieving the priorities in the Commissioner's strategic plan. Progress reports are also provided to the Audit and Finance Committee (A&FC).

In 2015-16 core infrastructure projects were successfully completed so that the former CLEDS and OVPC could transition to one organisation.

The performance measures to report on CPDP's contribution to DPC's Public Sector Integrity output in Budget Paper Number 3 were changed in 2015-16 to reflect the scope of work of the Commissioner for Privacy and Data Protection. CPDP met or exceeded all of its 2015-16 targets (see Appendix C).

The Audit and Finance Committee (A&FC), established in 2015, met five times in 2015-16. The A&FC assists the Commissioner in fulfilling his responsibilities relating to accounting, risk profile, operational practices and controls. The A&FC also advises the Commissioner on strategic directions and initiatives.

Shared Services

A range of corporate support services is provided to the Commissioner by the Department of Premier and Cabinet, notably in the areas of human resources and financial management. The agreement between the two parties regarding service provision is contained in a Memorandum of Understanding.

Communications and Publications

The Commissioner and staff had an active program of speaking engagements over the reporting period, principally around information sharing and the Victorian Protective Data Security Framework. This program covered Victorian public sector agencies and umbrella bodies, national and international forums.

Apart from technical, topic-specific publications, which are dealt with in more depth in the body of this report, the Commissioner launched a Twitter account and a mobile CPDP app.

The CPDP website was further developed and enhanced to provide greater information and tools for the public sector as well as privacy and data protection practitioners.

Occupational Health and Safety

The Commissioner aims to provide employees with a healthy and safe workplace. No time was lost in 2015-16 due to workplace injuries. The Office OH&S representative conducted a workplace hazard inspection and completed an office safety checklist during the year. No unacceptable OH&S risks were identified.

Workplace Relations

The Commissioner is advised on industrial relations issues by the Department of Premier and Cabinet. No industrial relations issues were registered or grievances received in the course of the reporting period.

Public Sector Conduct

Staff of the Commissioner for Privacy and Data Protection uphold the *Code of Conduct for Victorian Public Sector Employees*. No breaches of the *Code of Conduct* by the Commissioner's staff occurred in 2015-16.

Environmental Impacts

Under the terms of the Occupancy Agreement between the Department of Treasury and Finance/Shared Services Provider and the Commissioner for Privacy and Data Protection, the lessor has responsibility for the provision of energy, water and waste disposal for the premises occupied by the Commissioner. Energy and water are not metered separately. The principal environmental impacts of the Office of the Commissioner are therefore not included in this report.

Risk and Insurance Management

The Office of the Commissioner for Privacy and Data Protection has risk management processes in place which meet the requirements of the Victorian Government Risk Management Framework 2015, including the Australian/New Zealand Risk Standard AS/NZS ISO 31000:2009. Risk processes include regular reporting and review, an organisational risk management strategy, a risk register and a risk treatment action plan.

CPDP's Business Continuity Plan is regularly reviewed and tested.

CPDP's insurance is arranged with the VMIA, reviewed annually and considered as part of CPDP's risk management procedures.

The Commissioner's risk and insurance management attestation can be found at Appendix B.

Freedom of Information

The Commissioner received no Freedom of Information requests in 2015-16.

The Commissioner maintains copies of all reviews undertaken by his office and relevant working papers and correspondence. Due to the nature of the functions of the office, particularly with regard to public sector information security and law enforcement data, the Commissioner holds much information that would be considered exempt material under the *Freedom of Information Act 1*

Consultancies

Consultancy expenditure

Details of consultancies (valued at \$10,000 or greater)

In 2015-16 there were seven consultancies where the total fees payable to the consultants were \$10,000 or greater. The total expenditure incurred during 2015-16 in relation to these consultancies is \$146,532.82 (excluding GST). Details of individual consultancies are outlined below.

Name of Consultancy Firm	Purpose of Consultancy	Approved project fees (excl. GST)	Expenditure 2015-16 (excl. GST)
Senate shj	CPDP Stakeholder Engagement Strategy	\$20,000.00	\$20,000.00
Senate shj	CPDP Engagement and Communication Plan	\$25,000.00	\$25,000.00
Senate shj	CPDP Engagement and Communication Plan - Client Liaison	\$4,450.00	\$4,450.00
Diacher Pty Ltd	Review of CPDP Enquiries and Complaints Handling	\$33,750.00	\$6,750.00
KPMG	Review of VICPOL Security Incident Management framework and procedures review	\$90,703.64	\$45,351.82
EY Sweeney	Data coding for VICPOL survey	\$12,781.00	\$12,781.00
Sandra Beanham & Associates	VICPOL Survey consultation	\$32,200.00	\$32,200.00

Details of consultancies under \$10,000

In 2015-16, there were 5 consultancies engaged during the year where the total fees payable to the individual consultancies was less than \$10,000. The total expenditure incurred during 2015-16 in relation to these consultancies was \$24,570 (excluding GST).

Information and Communication Technology Expenditure

For the 2015-16 reporting period, CPDP had a total ICT expenditure of \$341,949 with details shown below.

(\$ thousand)			
Business As Usual (BAU) ICT expenditure	Non-Business As Usual (non-BAU) ICT expenditure.	Operational expenditure	Capital expenditure
(Total)	(Total = Operational expenditure and Capital Expenditure)		
168,673	173,276	145,533	27,744

ICT expenditure refers to the CPDP's costs in providing business enabling ICT services. It comprises Business As Usual (BAU) ICT expenditure and Non Business As Usual (Non BAU) ICT expenditure. Non BAU ICT expenditure relates to extending or enhancing the CPDP's current ICT capabilities. BAU ICT expenditure is all remaining ICT expenditure which primarily relates to ongoing activities to operate and maintain the current ICT capability.

Overseas Travel

The Commissioner and Assistant Commissioner Strategic Privacy conducted a series of meetings with the New Zealand Privacy Commissioner in July 2015.

The Assistant Commissioner Strategic Privacy also attended the meeting of the Australasia Pacific Privacy Association in Macau and the 17th annual Privacy and Security Conference in Canada.

Major Contracts

The Commissioner did not enter into any contracts valued at more than \$10 million in 2015-16.

Protected Disclosures

The Commissioner received no disclosures made under the *Protected Disclosures Act 2012* during 2015-16.

Gifts, Benefits and Hospitality

The Commissioner maintains a register of gifts, benefits and hospitality. No declarable items were registered in 2015-16.

Statement of Availability of Other Information

The Directions of the Minister for Finance pursuant to the *Financial Management Act 1994* require a range of information to be prepared for the reporting period. The relevant information is included in this report, with the exception of a statement that declarations of pecuniary interests have been duly completed by all relevant officers, which is held by the Commissioner and is available on request to the relevant Minister, Members of Parliament and the public (subject to Freedom of Information requirements, if applicable).



Annual Financial Statements 2015-16

Office of the Commissioner for Privacy and Data Protection

Annual Financial Statements 2015-16

Contents.....	Page
Accountable Officer's and Chief Finance and Accounting Officer's Declaration	46
Comprehensive operating statement.....	47
Balance sheet.....	48
Statement of changes in equity	49
Cash flow statement.....	50
Notes to the financial statements for the financial period ending 30 June 2016	51
Note 1. Summary of significant accounting policies.....	51
Note 2. Prior period correction.....	61
Note 3. Expenses from transactions.....	62
Note 4. Other economic flows included in net result	62
Note 5. Receivables.....	63
Note 6. Property, plant and equipment	63
Note 7. Intangible assets.....	65
Note 8. Payables.....	66
Note 9. Provisions.....	66
Note 10. Leases	67
Note 11. Superannuation.....	67
Note 12. Commitments for expenditure.....	68
Note 13. Contingent assets and contingent liabilities	68
Note 14. Financial instruments	68
Note 15. Cash flow information	70
Note 16. Responsible persons	71
Note 17. Remuneration of executives.....	71
Note 18. Remuneration of auditors.....	71
Note 19. Subsequent events	71
Note 20. Economic Dependency.....	72
Note 21. Glossary of terms	72

Accountable Officer's and Chief Finance and Accounting Officer's Declaration

The attached financial statements for the Office of the Commissioner for Privacy and Data Protection have been prepared in accordance with Direction 4.2 of the *Standing Directions* of the Minister for Finance under *Financial Management Act 1994*, applicable Financial Reporting Directions, Australian Accounting Standards including Interpretations, and other mandatory professional reporting requirements.

We further state that, in our opinion, the information set out in the comprehensive operating statement, balance sheet, statement of changes in equity, cash flow statement and accompanying notes, presents fairly the financial transactions during the period ended 30 June 2016 and financial position of the Office of the Commissioner for Privacy and Data Protection at 30 June 2016.

At the time of signing, we are not aware of any circumstances which would render any particulars included in the financial statements to be misleading or inaccurate.

We authorise the attached financial statements for issue on 19 September 2016.



David Watts
Commissioner for Privacy and Data Protection
Melbourne
19 September 2016



Ingrid Klein
Chief Financial Officer
Melbourne
19 September 2016

Comprehensive operating statement

	Notes	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Income from transactions			
Grants from State Government		3,865,768	3,796,432
Resources received free of charge		-	234,410
Other income		-	135,374
Total income from transactions		3,865,768	4,166,216
Expenses from transactions			
Employee expenses	3(a)	2,844,821	2,417,000
Supplies and services	3(b)	1,637,028	1,070,425
Depreciation and amortisation	3(c)	75,613	54,823
Total expenses from transactions		4,557,462	3,542,248
Net result from transactions (net operating balance)		(691,694)	623,968
Other economic flows included in net result			
Other gains/(losses) from other economic flows	4	(19,233)	(1,399)
Total other economic flows included in net result		(19,233)	(1,399)
Net result		(710,927)	622,569
Other economic flows - other comprehensive income		-	-
Total other economic flows - other comprehensive income		-	-
Comprehensive result		(710,927)	622,569

The above comprehensive operating statement should be read in conjunction with the accompanying notes.

Balance sheet

as at 30 June 2016

	Notes	2016 \$	2015 Restated \$
Assets			
Financial assets			
Receivables	5	1,098,644	1,720,209
Prepayments		29,234	80,000
Total financial assets		1,127,878	1,800,209
Non-financial assets			
Property, plant and equipment	6	212,078	272,693
Intangible assets	7	22,500	37,500
Total non-financial assets		234,578	310,193
Total assets		1,362,456	2,110,402
Liabilities			
Payables	8	583,150	605,406
Provisions	9	794,693	809,456
Total liabilities		1,377,843	1,414,862
Net assets/(liabilities)		(15,387)	695,540
Equity			
Accumulated surplus		(88,358)	622,569
Contributed capital		72,971	72,971
Net worth		(15,387)	695,540
Commitments for expenditure	12		
Contingent assets and contingent liabilities	13		

The above balance sheet should be read in conjunction with the accompanying notes.

Statement of changes in equity

	Accumulated Surplus \$	Contributions by owners \$	Total \$
Balance at 17 September 2014	-	-	-
Net result for the period (Restated)	622,569	-	622,569
Net asset transfers through contributed capital	-	72,971	72,971
Balance at 30 June 2015	622,569	72,971	695,540
Net result for the period	(710,927)	-	(710,927)
Balance at 30 June 2016	(88,358)	72,971	(15,387)

The above statement of changes in equity should be read in conjunction with the accompanying notes.

Cash flow statement

	Notes	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Cash flows from operating activities			
Receipts from Government		4,678,619	2,256,176
Payments to suppliers		(1,824,867)	(558,303)
Payments to employees		(2,853,752)	(1,597,467)
Net cash flows from operating activities	15(b)	-	100,406
Cash flows from investing activities			
Purchases of non-financial assets		-	(100,406)
Net cash flows used in investing activities		-	(100,406)
Net increase/(decrease) in cash and cash equivalents		-	-
Cash and cash equivalents at the beginning of the financial period		-	-
Cash and cash equivalents at the end of the financial period	15(a)	-	-

The above cash flow statement should be read in conjunction with the accompanying notes.

Notes to the financial statements for the financial period ending 30 June 2016

Note 1. Summary of significant accounting policies

These annual financial statements represent the audited general purpose financial statements for the Office for Privacy and Data Protection (Office) for the year ended 30 June 2016. The purpose of the report is to provide users with information about the Office's stewardship of resources entrusted to it.

(a) Statement of compliance

These general purpose financial statements have been prepared in accordance with the *Financial Management Act 1994* (FMA) and applicable Australian Accounting Standards (AAS), which include Interpretations issued by the Australian Accounting Standards Board (AASB). In particular, they are presented in a manner consistent with the requirements of AASB 1049 *Whole of Government and General Government Sector Financial Reporting*.

Where appropriate, those AAS paragraphs applicable to not-for-profit entities have been applied.

Accounting policies are selected and applied in a manner which ensures that the resulting financial information satisfies the concepts of relevance and reliability, thereby ensuring that the substance of the underlying transactions or other events is reported.

To gain a better understanding of the terminology used in this report, a glossary of terms can be found in Note 21.

These annual financial statements were authorised for issue by the Commissioner on 19 September 2016.

(b) Basis of accounting preparation and measurement

The accrual basis of accounting has been applied in the preparation of these financial statements whereby assets, liabilities, equity, income and expenses are recognised in the reporting period to which they relate, regardless of when cash is received or paid.

Judgements, estimates and assumptions are required to be made about the carrying values of assets and liabilities that are not readily apparent from other sources. The estimates and associated assumptions are based on professional judgements derived from historical experience and various other factors that are believed to be reasonable under the circumstances. Actual results may differ from these estimates.

Revisions to accounting estimates are recognised in the period in which the estimate is revised and also in future periods that are affected by the revision. Judgements and assumptions made by management in the application of AASs that have significant effects on the financial statements and estimates relate to:

- the fair value of plant and equipment (refer to Note 1(j));
- assumptions for employee benefit provisions based on likely tenure of existing staff, patterns of leave claims, future salary movements and future discount rates (refer Note 1(k));
- useful lives of plant and equipment (refer to Note 1(f)); and
- superannuation expense (refer to Note 1(f)).

These financial statements are presented in Australian dollars, and prepared in accordance with the historical cost convention, except where noted.

Consistent with AASB 13 *Fair Value Measurement*, the Office determines the policies and procedures for both recurring fair value measurements such as property, plant and equipment in accordance with the requirements of AASB 13 and the relevant Financial Reporting Directions.

All assets and liabilities for which fair value is measured or disclosed in the financial statements are categorised within the fair value hierarchy, described as follows, based on the lowest level input that is significant to the fair value measurement as a whole:

- Level 1 – Quoted (unadjusted) market prices in active markets for identical assets or liabilities
- Level 2 – Valuation techniques for which the lowest level input that is significant to the fair value measurement is directly or indirectly observable; and
- Level 3 – Valuation techniques for which the lowest level input that is significant to the fair value measurement is unobservable.

For the purpose of fair value disclosures, the Office has determined classes of assets and liabilities on the basis of the nature, characteristics and risks of the asset or liability and the level of the fair value hierarchy as explained above.

In addition, the Office determines whether transfers have occurred between levels in the hierarchy by reassessing categorisation (based on the lowest level input that is significant to the fair value measurement as a whole) at the end of each reporting period.

(c) Reporting entity

The financial statements cover the Office as an individual reporting entity.

The financial statements include all activities of the Office.

Its principal address is:

Level 6
121 Exhibition Street
Melbourne VIC 3000

Enabling legislation (*Privacy and Data Protection Act 2014*)

The Office is a department established under Part 6(1)(f) of the *Public Administration Act 2004* and is preparing this report in accordance with the *Privacy and Data Protection Act 2014* (the Act) under Division 3, Section 116. The Office is operating under the auspices of the Department of Premier and Cabinet and reporting to Parliament through the Special Minister of State. The Office's purposes, functions, powers and duties are set out in Part 1 and Part 3 of the Act.

Objectives and Funding

The main functions of the Office of the Commissioner for Privacy and Data Protection, under the Act, are:

- to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
- to balance the public interest in promoting open access to public sector information with the public interest in protecting its security;
- to promote awareness of responsible personal information handling practices in the public sector;
- to promote the responsible and transparent handling of personal information in the public sector;
- to promote responsible data security practices in the public sector.

The Office is funded for the provision of outputs consistent with its statutory functions. Funds are from accrual-based grants derived from monies appropriated annually by Parliament through the Department of Premier and Cabinet.

(d) Scope and presentation of financial statements

Comprehensive operating statement

The comprehensive operating statement comprises three components, being 'net result from transactions' (or termed as 'net operating balance'), 'other economic flows included in net result', as well as 'other economic flows – other comprehensive income'. The sum of the former two represents the net result.

The net result is equivalent to profit or loss derived in accordance with AASs.

'Other economic flows' are changes arising from market remeasurements. They include:

- gains and losses from disposals of non-financial assets;
- revaluations and impairments of non-financial physical and tangible assets; and
- the revaluation of the present value of leave liabilities due to changes in bond interest rates.

This classification is consistent with the whole of government reporting format and is allowed under AASB 101 *Presentation of Financial Statements*.

Balance sheet

Assets and liabilities are presented in liquidity order with assets aggregated into financial assets and non-financial assets.

Current and non-current assets and liabilities (non-current being those assets or liabilities expected to be recovered or settled beyond 12 months except for the provisions of employee benefits, which are classified as current liabilities if the Inspectorate does not have the unconditional right to defer the settlement of the liabilities within 12 months after the end of the reporting period) are disclosed in the notes, where relevant.

Cash flow statement

Cash flows are classified according to whether or not they arise from operating, investing, or financing activities. This classification is consistent with requirements under AASB 107 *Statement of Cash Flows*.

Statement of changes in equity

The statement of changes in equity presents reconciliations of each non-owner and owner changes in equity from opening balance at the beginning of the reporting period to the closing balance at the end of the reporting period. It also shows separately changes due to amounts recognised in the 'comprehensive result' and amounts recognised in 'other economic flows - other movements in equity' related to 'transactions with owner in its capacity as owner'.

(e) Income from transactions

Income is recognised to the extent that it is probable that the economic benefits will flow to the entity and the income can be reliably measured at fair value.

Grants

Income from grants (other than contribution by owners) is recognised when the Office obtains control over the contribution.

Fair value of assets and services received free of charge or for nominal consideration

Contributions of resources received free of charge or for nominal consideration are recognised at fair value when control is obtained over them, irrespective of whether these contributions are subject to restrictions or conditions over their use. Contributions in the form of services are only recognised when a fair value can be reliably determined and the services would have been purchased if not received as a donation.

The Department of Premier and Cabinet has been centrally funded for services it provides to the Office. These services are not recognised in the financial statements of the Office as their fair values cannot be reliably determined. The services that are utilised include the use of financial systems, payroll systems, accounts payable, asset register and IT network.

(f) Expenses from transactions

Expenses from transactions are recognised as they are incurred and reported in the financial period to which they relate.

Employee expenses

Refer to the section in Notes 1(k) regarding employee benefits.

These expenses include all costs related to employment, including wages and salaries, superannuation, fringe benefits tax, leave entitlements, redundancy payments and WorkCover premiums.

The amount recognised in the comprehensive operating statement for superannuation expense is the employer contributions for members of both defined benefit and defined contribution superannuation plans that are paid or payable to these plans during the reporting period.

The Department of Treasury and Finance (DTF), in their annual financial statements, disclose on behalf of the State as the sponsoring employer, the net defined benefit cost related to the members of these plans as an administered liability. Refer to DTF's Annual Financial Statements for more detailed disclosures in relation to these plans.

Depreciation and amortisation

Depreciation is generally calculated on a straight-line basis, at rates that allocate the asset's value, less any estimated residual value, over its estimated useful life.

Intangible assets with finite useful lives are depreciated as an expense on a straight line basis over the asset's useful life.

Refer to Note 1(j) for the amortisation policy for leasehold improvements.

The estimated useful lives, residual values and depreciation method are reviewed at the end of each annual reporting period, and adjustments made where appropriate.

The following are typical estimated useful lives for the different asset classes.

- plant, computers and communications equipment - 3-10 years
- leasehold improvements - 8 years
- software development and licence costs - 3 years

Supplies and services

Supplies and services costs are recognised as expenses in the reporting period in which they are incurred.

(g) Other economic flows included in the net result

Other economic flows measure the change in volume or value of assets or liabilities that do not result from transactions.

Net gain/(loss) on non-financial assets

Net gain/(loss) on non-financial assets and liabilities includes realised and unrealised gains and losses as follows:

Disposal of non-financial assets

Any gain or loss on the disposal of non-financial assets is recognised at the date of disposal and is determined after deducting from the proceeds the carrying value of the asset at that time.

Impairment of non-financial assets

All non-financial assets are assessed annually for impairment, as to whether their carrying value exceeds their recoverable amount and so require write downs, and whenever there is an indication that the asset may be impaired.

If there is an indication of impairment, the assets concerned are tested as to whether their carrying value exceeds their recoverable amount. Where an asset's carrying value exceeds its recoverable amount, the difference is written off as an other economic flow, except to the extent that the write-down can be debited to an asset revaluation surplus amount applicable to that class of asset.

If there is an indication that there has been a change in the estimate of an asset's recoverable amount since the last impairment loss was recognised, the carrying amount shall be increased to its recoverable amount. This reversal of the impairment loss occurs only to the extent that the asset's carrying amount does not exceed the carrying amount that would have been determined, net of depreciation or amortisation, if no impairment loss had been recognised in prior years.

It is deemed that, in the event of the loss or destruction of an asset, the future economic benefits arising from the use of the asset will be replaced unless a specific decision to the contrary has been made. The recoverable amount for most assets is measured at the higher of depreciated replacement cost and fair value less costs to sell. Recoverable amount for assets held primarily to generate net cash inflows is measured at the higher of the present value of future cash flows expected to be obtained from the asset and fair value less costs to sell.

Refer to Note 1(j) in relation to the recognition and measurement of non-financial assets.

Impairment of financial assets

At the end of each reporting period, the Office assesses whether there is objective evidence that a financial asset or group of financial assets is impaired. All financial instrument assets, except those measured at fair value through profit or loss, are subject to annual review for impairment.

Receivables are assessed for bad and doubtful debts on a regular basis. Those bad debts considered as written off by mutual consent are classified as a transaction expense. The allowance for doubtful receivables and bad debts not written off by mutual consent are adjusted as other economic flows.

Net gain/(loss) on financial instruments

Net gain/(loss) on financial instruments includes:

- realised and unrealised gains and losses from revaluations of financial instruments at fair value;
- impairment and reversal of impairment for financial instruments at amortised cost (refer to Note 1(h)); and
- disposals of financial assets.

Other gains/(losses) from other economic flows

Other gains/(losses) from other economic flows include the gains or losses from:

- the revaluation of the present value of the long service leave liability due to changes in the bond interest rates; and
- transfer of amounts from the reserves to accumulated surplus or net result due to disposal or derecognition or reclassification.

(h) Financial instruments

Financial instruments arise out of contractual agreements that give rise to a financial asset of one entity and a financial liability or equity instrument of another entity. Due to the nature of the Office's activities, certain financial assets and financial liabilities arise under statute rather than a contract. Such financial assets and financial liabilities do not meet the definition of financial instruments in AASB 132 *Financial Instruments: Presentation*. For example, statutory receivables arising from taxes, fines and penalties do not meet the definition of financial instruments as they do not arise under contract.

Where relevant, for note disclosure purposes, a distinction is made between those financial assets and financial liabilities that meet the definition of financial instruments in accordance with AASB 132 and those that do not.

The following refers to financial instruments unless otherwise stated.

Loans and receivables

Loans and receivables are financial instrument assets with fixed and determinable payments that are not quoted on an active market. These assets are initially recognised at fair value plus any directly attributable transaction costs. Subsequent to initial measurement, loans and receivables are measured at amortised cost using the effective interest method, less any impairment.

Loans and receivables category includes cash and deposits, term deposits with maturity greater than three months, trade receivables, loans and other receivables, but not statutory receivables.

Financial liabilities at amortised cost

Financial instrument liabilities are initially recognised on the date they are originated. They are initially measured at fair value plus any directly attributable transaction costs. Subsequent to initial recognition, these financial instruments are measured at amortised cost with any difference between the initial recognised amount and the redemption value being recognised in profit and loss over the period of the interest-bearing liability, using the effective interest rate method (refer to Note 21).

Financial instrument liabilities measured at amortised cost include all of the Office's contractual payables.

(i) Financial assets

Receivables

Receivables consist of:

- contractual receivables, such as debtors in relation to goods and services.
- statutory receivables, which include predominantly amounts owing from the Victorian Government.

Where applicable, contractual receivables are classified as financial instruments and categorised as loans and receivables (refer to Note 14 Financial Instruments for recognition and measurement). Statutory receivables are recognised and measured similarly to contractual receivables (except for impairment), but are not classified as financial instruments because they do not arise from a contract.

Receivables are subject to impairment testing as described above. A provision for doubtful receivables is recognised when there is objective evidence that the debts may not be collected, and bad debts are written off when identified.

(j) Non-financial assets

Plant and equipment

All non-financial physical assets are measured initially at cost and subsequently revalued at fair value less accumulated depreciation and impairment. Where an asset is acquired for no or nominal cost, the cost is its fair value at the date of acquisition. Assets transferred as part of a machinery of government change are transferred at their carrying amount.

Plant and equipment is held at fair value. The Office applies an individual asset capitalisation threshold of \$5,000. Individual acquisitions below this value are expensed.

Leasehold improvements

The cost of leasehold improvements is capitalised as an asset and depreciated over the shorter of the term of the lease or the estimated useful life of the improvements.

Intangible assets

Intangible assets are initially recognised at cost. Subsequently, intangible assets with finite useful lives are carried at cost less accumulated amortisation and accumulated impairment losses. Costs incurred subsequent to initial acquisition are capitalised when it is expected that additional future economic benefits will flow to the Office.

Prepayments

Prepayments represent payments in advance of receipt of goods or services or that part of expenditure made in one accounting period covering a term extending beyond that period.

(k) Liabilities

Payables

- Payables consist of:
 - contractual payables, such as accounts payable. Accounts payable represent liabilities for goods and services provided to the Office prior to the end of the financial year that are unpaid, and arise when the Office becomes obliged to make future payments in respect of the purchase of those goods and services; and
- statutory payables, such as goods and services tax and fringe benefits tax payables.

Contractual payables are classified as financial instruments and categorised as financial liabilities at amortised cost (refer to Note 8). Statutory payables are recognised and measured similarly to contractual payables, but are not classified as financial instruments and not included in the category of financial liabilities at amortised cost, because they do not arise from a contract.

Provisions

Provisions are recognised when the Office has a present obligation, the future sacrifice of economic benefits is probable, and the amount of the provision can be measured reliably.

The amount recognised as a provision is the best estimate of the consideration required to settle the present obligation at reporting period, taking into account the risks and uncertainties surrounding the obligation. Where a provision is measured using the cash flows estimated to settle the present obligation, its carrying amount is the present value of those cash flows, using discount rate that reflects the time value of money and risks specific to the provision.

When some or all of the economic benefits required to settle a provision are expected to be received from a third party, the receivable is recognised as an asset if it is virtually certain that recovery will be received and the amount of the receivable can be measured reliably.

Employee benefits

Provision is made for benefits accruing to employees in respect of wages and salaries, annual leave and long service leave for services rendered to the reporting date.

(i) Wages and salaries and annual leave

Liabilities for wages and salaries, including non monetary benefits annual leave and accumulating sick leave, are all recognised in the provision for employee benefits as 'current liabilities', because the Office does not have an unconditional right to defer settlements of these liabilities.

Depending on the expectation of the timing of settlement, liabilities for wages and salaries, annual leave and sick leave are measured at:

- undiscounted value if the Office expects to wholly settle within 12 months; or
- present value if the Office does not expect to wholly settle within 12 months.

(ii) Long service leave

Liability for long service leave (LSL) is recognised in the provision for employee benefits.

Unconditional LSL is disclosed in the notes to the financial statements as a current liability even where the Office does not expect to settle the liability within 12 months because it will not have the unconditional right to defer the settlement of the entitlement should an employee take leave within 12 months.

The components of this current LSL liability are measured at:

- undiscounted value if the Office expects to wholly settle within 12 months; and
- present value if the Office does not expect to wholly settle within 12 months.

Conditional LSL is disclosed as a non-current liability. There is an unconditional right to defer the settlement of the entitlement until the employee has completed the requisite years of service. This non-current LSL liability is measured at present value.

Any gain or loss following revaluation of the present value of non-current LSL liability is recognised as a transaction, except to the extent that a gain or loss arises due to changes in bond interest rates for which it is then recognised as an other economic flow (refer to Note 1(g)).

(iii) Termination benefits

Termination benefits are payable when employment is terminated before the normal retirement date, or when an employee decides to accept an offer of benefits in exchange for the termination of employment. The Office recognises termination benefits when it is demonstrably committed to either terminating the employment of current employees according to a detailed formal plan without possibility of withdrawal or providing termination benefits as a result of an offer made to encourage voluntary redundancy. Benefits falling due more than 12 months after the end of the reporting period are discounted to present value.

(l) Leases

A lease is a right to use an asset for an agreed period of time in exchange for payment.

Leases are classified at their inception as either operating or finance leases based on the economic substance of the agreement so as to reflect the risk and reward incidental to ownership. Leases of property, plant and equipment are classified as finance infrastructure leases whenever the terms of the lease transfer substantially all the risks and rewards of ownership from the lessor to the lessee. All other leases are classified as operating leases.

Operating leases

Operating lease payments, including any contingent rentals, are recognised as an expense in the comprehensive operating statement on a straight-line basis over the lease term, except where another systematic basis is more representative of the time pattern of the benefits derived from the use of the leased asset. The leased asset is not recognised in the balance sheet.

All incentives for the agreement of a new or renewed operating lease are recognised as an integral part of the net consideration agreed for the use of the leased asset, irrespective of the incentive's nature or form or the timing of payments.

In the event that lease incentives are received to enter into operating leases, the aggregate cost of incentives are recognised as a reduction of rental expense over the lease term on a straight-line basis, unless another systematic basis is more representative of the time pattern in which economic benefits from the leased asset are consumed.

(m) Equity

Consistent with the requirements of AASB1004 *Contributions*, contributions by owners (that is contributed capital and its repayment) are treated as equity transactions and, therefore, do not form part of the income and expenses of the Office.

Additions to net assets which have been designated as contributions by owners are recognised as contributed capital. Other transfers that are in the nature of contributions or distributions have also been designated as contributions by owners.

(n) Commitments

Commitments for future expenditure include operating and capital commitments arising from contracts. These commitments are disclosed by way of a note at their nominal value and exclusive of the goods and services tax (GST) payable. In addition, where it is considered appropriate and provides relevant information to users, the net present values of significant individual projects are stated. These future expenditures cease to be disclosed as commitments once the related liabilities are recognised in the balance sheet.

(o) Contingent assets and contingent liabilities

Contingent assets and contingent liabilities are not recognised in the balance sheet, but are disclosed by way of a note (refer to Note 13) and, if quantifiable, are measured at nominal value. Contingent assets and liabilities are presented inclusive of GST receivable or payable respectively.

(p) Accounting for the goods and services tax (GST)

Income, expenses and assets are recognised net of the amount of associated GST, except where the GST incurred is not recoverable from the taxation authority. In this case, the GST payable is recognised as part of the cost of acquisition of the asset or as part of the expense.

Receivables and payables are stated inclusive of the amount of GST receivable or payable. The net amount of GST recoverable from or payable to the taxation authority is included with other receivables or payables in the balance sheet.

Cash flows are presented on a gross basis. The GST components of cash flows arising from investing or financing activities which are recoverable from or payable to the taxation authority are presented as an operating cash flow.

(q) Events after the reporting period

Assets, liabilities, income or expenses arise from past transactions or other past events. Where the transactions result from an agreement between the Office and other parties, the transactions are only recognised when the agreement is irrevocable at or before the end of the reporting period. Adjustments are made to amounts recognised in the financial statements for events which occur between the end of the reporting period and the date when the financial statements are authorised for issue, where those events provide information about conditions which existed at the reporting date. Note disclosure is made about events between the end of the reporting period and the date the financial statements are authorised for issue where the events relate to conditions which arose after the end of the reporting period that are considered to be of material interest.

(r) Rounding

Amounts in the financial statements have been rounded to the nearest dollar.

(s) Australian Accounting Standards issued that are not yet effective

As at 30 June 2016, the following standards and interpretations (applicable to the Office) had been issued but were not mandatory for the 30 June 2016 reporting period. The Department of Treasury and Finance assesses the impact of these new standards and advises the Office of their applicability and early adoption where applicable.

AASB 9 *Financial Instruments*, applicable for reporting periods commencing 1 January 2018. The key changes include the simplified requirements for the classification and measurement of financial assets, a new hedging accounting model and a revised impairment loss model to recognise impairment losses earlier, as opposed to the current approach that recognises impairment only when incurred. While the Office's assessment has not identified any material impact arising from AASB 9, it will continue to be monitored and assessed.

AASB 2010-7 *Amendments to Australian Accounting Standards arising from AASB 9 (December 2010)*, applicable for reporting periods commencing 1 January 2018. The requirements for classifying and measuring financial liabilities were added to AASB 9. The existing requirements for the classification of financial liabilities and the ability to use the fair value option have been retained. However, where the fair value option is used for financial liabilities the change in fair value is accounted for as follows:

- the change in fair value attributable to changes in credit risk is presented in other comprehensive income; and
- other fair value changes are presented in profit or loss. If this approach creates or enlarges an accounting mismatch in the profit or loss, the effect of the changes in credit risk are also presented in profit or loss.

The Office's assessment has identified that the amendments are likely to result in earlier recognition of impairment losses and at more regular intervals.

AASB 2014-1 *Amendments to Australian Accounting Standards [Part E Financial Instruments]*, applicable for reporting periods commencing 1 January 2018. Amends various AASs to reflect the AASB's decision to defer the mandatory application date of AASB 9 to annual reporting periods beginning on or after 1 January 2018; as a consequence of Chapter 6; and to amend reduced disclosure requirements. This amending standard will defer the application period of AASB 9 to the 2018-19 reporting period in accordance with the transition requirements.

AASB 2014-7 *Amendments to Australian Accounting Standards* arising from AASB 9, applicable for reporting periods commencing 1 January 2018. Amends various AASs to incorporate the consequential amendments arising from the issuance of AASB 9. The Office's assessment has indicated that there will be no significant impact for the Office.

AASB 15 *Revenue from Contracts with Customers*, applicable for reporting periods commencing 1 January 2018. The core principle of AASB 15 requires an entity to recognise revenue when the entity satisfies a performance obligation by transferring a promised good or service to a customer. Note that amending standard AASB 2015-8 *Amendments to Australian Accounting Standards – Effective Date of AASB 15* has deferred the effective date of AASB 15 to annual reporting periods beginning on or after 1 January 2018, instead of 1 January 2017. The changes in revenue recognition

requirements in AASB 15 may result in changes to the timing and amount of revenue recorded in the financial statements. The Standard will also require additional disclosures on service revenue and contract modifications.

AASB 2014-5 *Amendments to Australian Accounting Standards* arising from AASB 15, applicable 1 Jan 2017, except amendments to AASB 9 (Dec 2009) and AASB 9 (Dec 2010) apply from 1 Jan 2018. Amends the measurement of trade receivables and the recognition of dividends. Trade receivables, that do not have a significant financing component, are to be measured at their transaction price, at initial recognition. The Office's assessment has indicated that there will be no significant impact for the Office.

AASB 16 *Leases*, applicable for reporting periods commencing 1 January 2019. The key changes introduced by AASB 16 include the recognition of most operating leases (which are currently not recognised) on balance sheet. The Office's assessment has indicated that as most operating leases will come on balance sheet, recognition of lease assets and lease liabilities will cause net debt to increase. Depreciation of lease assets and interest on lease liabilities will be recognised in the income statement with marginal impact on the operating surplus. The amounts of cash paid for the principal portion of the lease liability will be presented within financing activities and the amounts paid for the interest portion will be presented within operating activities in the cash flow statement.

AASB 2015-1 *Amendments to Australian Accounting Standards – Annual Improvements to Australian Accounting Standards 2012-2014 Cycle [AASB 1, AASB 2, AASB 3, AASB 5, AASB 7, AASB 11, AASB 110, AASB 119, AASB 121, AASB 133, AASB 134, AASB 137 & AASB 140]*, applicable for reporting periods commencing 1 January 2016. Amends the methods of disposal in AASB 5 *Non-current assets held for sale and discontinued operations*. Amends AASB 7 *Financial Instruments* by including further guidance on servicing contracts. The assessment has indicated that when an asset (or disposal group) is reclassified from 'held to sale' to 'held for distribution', or vice versa, the asset does not have to be reinstated in the financial statements. Entities will be required to disclose all types of continuing involvement the entity still has when transferring a financial asset to a third party under conditions which allow it to derecognise the asset.

AASB 2015-6 *Amendments to Australian Accounting Standards – Extending Related Party Disclosures to Not-for-Profit Public Sector Entities [AASB 10, AASB 124 & AASB 1049]*, applicable for reporting periods commencing 1 January 2016. AASB 2015-6 extends the scope of AASB 124 *Related Party Disclosures* to not-for-profit public sector entities. Guidance has been included to assist the application of the Standard by not-for-profit public sector entities. The amending standard will result in extended disclosures on the entity's key management personnel, and the related party transactions.

Note 2 Prior period correction

In 2014-15 the Office recognised an accrual for 6 months operating lease expense for the lease of 121 Exhibition Street Melbourne of \$160,000 in error. This error had the effect of overstating expenses for the year by \$160,000 and understating accumulated surplus by \$160,000.

In 2014-15 the Office recognised a prepayment for fitout of leased premises as a work in progress asset in error. This error had the effect overstating property, plant and equipment by \$80,000 and understating prepayments by \$80,000.

These over accrual and prepayment amounts have been corrected by restating each of the affected financial statement line items for the year ended 30 June 2015 as below:

	As published 2015	Effect of change 2015	Restated 2015
Comprehensive operating statement			
Supplies and services	1,230,425	(160,000)	1,070,425
Net result from transactions	463,968	(160,000)	623,968
Net result	462,569	(160,000)	622,569
Comprehensive result	462,569	(160,000)	622,569
Balance sheet			
Prepayments	-	80,000	80,000
Total financial assets	1,720,209	80,000	1,800,209
Property, plant and equipment	352,693	(80,000)	272,693
Total non-financial assets	390,193	(80,000)	310,193
Payables	765,406	(160,000)	605,406
Total liabilities	1,574,862	(160,000)	1,414,862
Net assets	535,540	160,000	695,540
Accumulated surplus	462,569	(160,000)	622,569
Net worth	535,540	(160,000)	695,540
Statement of changes in equity			
Net result for the period	462,569	160,000	622,569
Balance at 30 June 2015	462,569	160,000	622,569
Cash flow statement			
Payments to suppliers	(478,303)	(80,000)	(558,303)
Net cash flows from operating activities	180,406	(80,000)	100,406
Purchases of non-financial assets	(180,406)	80,000	(100,406)
Net cash flows used in investing activities	(180,406)	80,000	(100,406)

Note 3. Expenses from transactions

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Expenses from transactions includes:		
(a) Employee expenses		
Salaries and wages	2,219,273	1,871,029
Annual leave and long service leave	287,606	300,821
Post employment benefits		
Defined contribution superannuation expense	188,531	145,492
Defined benefit superannuation expense	17,766	10,971
Other on-costs (fringe benefits tax, payroll tax and WorkCover levy)	131,645	88,687
Total employee expenses	2,844,821	2,417,000
(b) Supplies and services		
Professional services	628,844	178,558
Information technology	301,175	291,156
Lease rentals and outgoings	373,586	335,146
Other	333,423	265,565
Total supplies and services	1,637,028	1,070,425
(c) Depreciation and amortisation		
Depreciation - plant, computers and communications equipment	23,886	23,083
Amortisation - building leasehold improvements	36,727	24,240
Amortisation - software development and licence costs	15,000	7,500
Total depreciation and amortisation	75,613	54,823

Note 4. Other economic flows included in net result

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Other gains/(losses) from other economic flows		
Net gain/(loss) arising from revaluation of leave liabilities ⁽ⁱ⁾	(19,233)	(1,399)
Total other gains/(losses) from other economic flows	(19,233)	(1,399)

Note:

(i) Revaluation gain/(loss) due to changes in government bond rates.

Note 5. Receivables

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Current receivables		
Statutory		
GST recoverable	49,242	1,808
Amounts receivable from Victorian government departments ⁽ⁱ⁾	1,022,731	1,668,061
Total current receivables	1,071,973	1,669,869
Non-current receivables		
Statutory		
Amounts receivable from Victorian government departments ⁽ⁱ⁾	26,671	50,340
Total non-current receivables	26,671	50,340
Total receivables	1,098,644	1,720,209

(i) The amounts receivable from Victorian government departments represent funding for all commitments incurred through the appropriations and are drawn down as the commitments fall due.

Note 6. Property, plant and equipment

Gross carrying amounts and accumulated depreciation

	Gross carrying amount		Accumulated depreciation		Net carrying amount	
	2016 \$	2015 \$	2016 \$	2015 \$	2016 \$	2015 \$
Leasehold improvements at cost	226,071	226,071	(72,108)	(35,380)	153,963	190,691
Plant, computers and communications equipment at fair value	93,944	93,945	(35,829)	(11,943)	58,115	82,002
Total property, plant and equipment	320,015	400,016	107,937)	(47,323)	212,078	272,693

Movements in carrying amounts

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
	Leasehold improvements at cost	Leasehold improvements at cost
Opening balance	190,691	-
Additions	-	55,406
Transfers free of charge	-	135,482
Reclassifications	-	24,043
Amortisation	(36,728)	(24,240)
Closing balance	153,963	190,691
	Plant, computers and communications equipment at fair value	Plant, computers and communications equipment at fair value
Opening balance	82,002	-
Transfers free of charge	-	98,928
Transfers through contributed capital	-	30,200
Reclassifications	-	(24,043)
Depreciation	(23,887)	(23,083)
Closing balance	58,115	82,002

Plant, computers and communications equipment

Plant, computers and communications equipment is held at fair value. When such equipment is specialised in use, such that it is rarely sold other than as part of a going concern, fair value is determined using the depreciation replacement cost method.

There were no changes in valuation techniques throughout the period to 30 June 2016.

For all assets measured at fair value, the current use is considered the highest and best use.

Fair value measurement hierarchy for assets as at 30 June 2016

	Carrying amount \$	Fair value measurement, using:		
		Level 1 ⁽ⁱ⁾ \$	Level 2 ⁽ⁱ⁾ \$	Level 3 ⁽ⁱ⁾ \$
Plant, computers and communications equipment at fair value	58,115	-	-	58,115
Total of property, plant and equipment at fair value	58,115	-	-	58,115

(i) Classified in accordance with the fair value hierarchy, see Note 1(b).

Description of significant unobservable inputs to Level 3 valuations

	Valuation technique ⁽ⁱ⁾	Significant unobservable inputs ⁽ⁱ⁾
Plant, computers and communications equipment	Depreciated replacement cost	Cost per unit Useful life of equipment

(i) Plant, computers and communications equipment is held at fair value. When such assets are specialised in use, such that they are rarely sold other than as part of a going concern, fair value is determined using the depreciated replacement cost method.

Note 7. Intangible assets**Gross carrying amounts and accumulated amortisation**

	Gross carrying amount		Accumulated amortisation		Net carrying amount	
	2016 \$	2015 \$	2016 \$	2015 \$	2016 \$	2015 \$
Software development and licence costs at cost	45,000	45,000	(22,500)	(7,500)	22,500	37,500
Total intangible assets	45,000	45,000	(22,500)	(7,500)	22,500	37,500

Movements in carrying amounts

	2016 \$	2015 \$
Opening balance	37,500	-
Additions	-	45,000
Amortisation	(15,000)	(7,500)
Closing balance	22,500	37,500

Note 8. Payables

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Current payables		
Contractual		
Supplies and services	541,660	584,181
Other payables	33,133	19,142
	574,793	603,323
Statutory		
Amounts payable to other government agencies	8,357	2,083
	8,357	2,083
Total payables	583,150	605,406

(a) Maturity analysis of contractual payables

Refer to Note 14 for the maturity analysis of contractual payables.

(b) Nature and extent of risk arising from contractual payables

Refer to Note 14 for the nature and extent of risks arising from contractual payables.

Note 9. Provisions

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Current provisions		
Employee benefits - annual leave		
Unconditional and expected to settle within 12 months	196,670	192,135
Unconditional and expected to settle after 12 months	29,727	50,909
Employee benefits - long service leave:		
Unconditional and expected to settle within 12 months	93,427	90,313
Unconditional and expected to settle after 12 months	448,198	425,759
Total current provisions	768,022	759,116
Non-current provisions		
Employee benefits - long service leave	26,671	50,340
Total non-current provisions	26,671	50,340
Total provisions	794,693	809,456

Note 10. Leases

Operating leases

Commitments under a non-cancellable operating lease at the reporting date are as follows:

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Not longer than 1 year	401,788	384,944
Longer than 1 year and not longer than 5 years	1,773,388	1,695,874
Longer than 5 years	488,278	950,369
Total commitments	2,663,454	3,031,187

Leasing arrangements

The Exhibition Street, Melbourne office facilities have an initial lease term of eight years, terminating as at 30 June 2022, with an option to extend for a further five years. The Office does not have an option to purchase the leased asset at the expiry of the lease period.

Note 11. Superannuation

Employees of the Office are entitled to receive superannuation benefits and the Office contributes to both defined benefit and defined contribution plans. The defined benefit plans provide benefits based on years of service and final average salary.

The Office does not recognise any defined benefit liability in respect of the plans because the entity has no legal or constructive obligation to pay future benefits relating to its employees; its only obligation is to pay superannuation contributions as they fall due. The Department of Treasury and Finance recognises and discloses the State's defined benefit liabilities in its disclosure for administered items.

However, superannuation contributions paid or payable for the reporting period are included as part of employee benefits in the comprehensive operating statement of the Office.

The name, details and amounts expensed in relation to the major employee superannuation funds and contributions made by the Office are as follows:

Fund	Paid contribution for the year		Contribution outstanding at year end	
	2016 \$	17 September 2014 to 30 June 2015 \$	2016 \$	17 September 2014 to 30 June 2015 \$
Defined benefit funds				
State Superannuation Fund	17,773	10,971	-	-
Defined contribution funds				
VicSuper	128,237	124,258	-	-
Other	56,976	21,234	-	-
Total	202,986	156,463	-	-

Note 12. Commitments for expenditure

Apart from operating lease commitments (refer Note 10), there were no commitments for capital or other expenditure at 30 June 2015 or 30 June 2016.

Note 13. Contingent assets and contingent liabilities

There were no contingent assets or contingent liabilities at 30 June 2015 or 30 June 2016.

Note 14. Financial instruments

(a) Financial risk management objectives and policies

The Office's financial instruments comprise:

- receivables (excluding statutory receivables); and
- payables (excluding statutory payables).

Details of the significant accounting policies and methods adopted, including the criteria for recognition, the basis of measurement, and the basis on which expenses and income are recognised, with respect to each class of financial asset, financial liability and equity instrument above are disclosed in Note 1 to the financial statements.

The main purpose in holding financial instruments is to prudentially manage the Office's financial risks in the government policy parameters.

The carrying amounts of the Office's contractual financial assets and contractual financial liabilities by category are set out below:

Categorisation of financial instruments

	Contractual financial liabilities at amortised cost
2016	\$
Contractual financial liabilities	
Payables ⁽ⁱ⁾	574,793
Total contractual financial liabilities	574,793
2015	\$
Contractual financial liabilities	
Payables ⁽ⁱ⁾	603,323
Total contractual financial liabilities	603,323

(i) The total amounts disclosed here exclude statutory amounts (e.g. amounts owing from Victorian Government and taxes payable).

(b) Credit risk

Credit risk associated with the Office's financial assets is minimal because the main debtor is the Victorian Government. For debtors other than the Government, it is the Office's policy to only deal with entities with high credit ratings of a minimum triple B rating and to obtain sufficient collateral or credit enhancements, where appropriate.

(c) Liquidity risk

Liquidity risk is the risk that the Office would be unable to meet its financial obligations as and when they fall due. The Office operates under the Government fair payments policy of settling financial obligations within 30 days and, in the event of a dispute, make payments within 30 days from the date of resolution.

The Office's exposure to liquidity risk is deemed insignificant based on the current assessment of risk.

The following table discloses the contractual maturity analysis for the Office's contractual financial liabilities.

Maturity analysis of contractual financial liabilities ⁽ⁱ⁾

	Carrying amount \$	Nominal amount \$	Maturity dates ⁽ⁱ⁾				
			Less than 1 month \$	1 month to 3 months \$	3 months to 1 year \$	1 year to 5 years \$	5+ years \$
2016							
Payables ⁽ⁱⁱ⁾	574,793	574,793	574,793	-	-	-	-
	574,793	574,793	574,793	-	-	-	-
2015							
Payables ⁽ⁱⁱ⁾	603,323	603,323	603,323	-	-	-	-
	603,323	603,323	603,323	-	-	-	-

(i) Maturity analysis is presented using the contractual undiscounted cash flows.

(ii) The carrying amounts disclosed exclude statutory amounts (e.g. FBT payable).

(d) Market risk

The Office's exposure to market risk is deemed insignificant based on current assessment of risk.

(e) Fair Value

The fair values and net fair values of financial instrument assets and liabilities are determined as follows:

- Level 1 – the fair value of financial instruments with standard terms and conditions and traded in active liquid markets are determined with reference to quoted market prices;
- Level 2 – the fair value is determined using inputs other than quoted prices that are observable for the financial asset or liability, either directly or indirectly; and
- Level 3 – the fair value is determined in accordance with generally accepted pricing models based on discounted cash flow analysis using unobservable market inputs.

The Office considers that the carrying amount of financial assets and financial liabilities recorded in the financial statements to be a fair approximation of their fair values, because of the short term nature of the financial instruments and the expectation that they will be paid in full.

Note 15. Cash flow information**(a) Reconciliation of cash and cash equivalents**

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Total cash and cash equivalents disclosed in the balance sheet ⁽ⁱ⁾	-	-
Balance as per cash flow statement	-	-

Note:

(i) Due to the State of Victoria's investment policy and government funding arrangements, government departments and agencies generally do not hold a large cash reserve in their bank accounts. Cash received by a department and agencies from the generation of revenue is generally paid into the State's bank account, known as the Public Account. Similarly, any departmental or agency expenditure, including those in the form of cheques drawn by the Office for the payment of goods and services to its suppliers and creditors, are made via the Public Account. The process is such that the Public Account would remit cash required for the amount drawn on the cheques. This remittance by the Public Account occurs upon the presentation of the cheques by the Office's suppliers or creditors.

(b) Reconciliation of net result for the period

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Net result for the period	(710,927)	622,569
Non-cash movements		
Depreciation and amortisation of non-current assets	75,613	54,823
Resources received free of charge	-	(234,410)
Movements in assets and liabilities (net of effects of restructuring)		
(Increase)/decrease in receivables	621,566	(1,379,190)
(Increase)/decrease in prepayments	50,766	(80,000)
(Decrease)/increase in payables	(22,255)	578,642
(Decrease)/increase in provisions	(14,763)	537,972
Net cash flows from operating activities	-	100,406

Note 16. Responsible persons

In accordance with the Ministerial Directions issued by the Minister for Finance under the *Financial Management Act 1994*, the following disclosures are made regarding responsible persons for the reporting period.

Names

The persons who held the positions of Ministers and Accountable Officers in the Office are as follows:

The Hon Gavin Jennings MP Special Minister of State

David Watts Commissioner

The Hon Daniel Andrews MP acted in the office of the Special Minister of State in the absence of the Hon Gavin Jennings MLC.

Remuneration

Remuneration received or receivable by the Accountable Officer in connection with the management of the Office during the reporting period (to 30 June 2016) was in the range: \$300,000 to \$309,999

Amounts relating to Ministers are reported in the financial statements of the Department of Premier and Cabinet. For information regarding related party transactions of ministers, the register of members' interests is publicly available from: www.parliament.vic.gov.au/publications/register-of-interests

Other transactions

Other related transactions and loans requiring disclosure under the Directions of the Minister for Finance have been considered and there are no matters to report.

Note 17. Remuneration of executives

Other than the Accountable Officer (refer above), there were no executive officers within the Office during the reporting period.

No contractors held significant management responsibilities within the Office.

Note 18. Remuneration of auditors

	2016 \$	17 September 2014 to 30 June 2015 (Restated) \$
Victorian Auditor-General's Office		
Audit of the Victorian Privacy Commissioner 2014-15	1,500	-
Audit of the financial statements	15,500	15,000
	17,000	15,000

Note 19. Subsequent events

No events that should be reported have occurred after the end of the financial period.

Note 20. Economic Dependency

The Commissioner for Privacy and Data Protection is dependent upon the State of Victoria, via the Department of Premier and Cabinet, for the funding of its operations. At the date of this report management has no reason to believe that this financial support will not continue.

Note 21. Glossary of terms

Commitments

Commitments include those operating, capital and other outsourcing commitments arising from non-cancellable contractual or statutory sources.

Comprehensive result

The net result of all items of income and expense recognised for the period. It is the aggregate of operating result and other comprehensive income.

Depreciation

Depreciation is an expense that arises from the consumption through wear or time of a produced physical or intangible asset. This expense is classified as a 'transaction' and so reduces the 'net result from transactions'.

Effective interest method

The effective interest method is used to calculate the amortised cost of a financial asset and of allocating interest income over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash receipts through the expected life of the financial instrument, or, where appropriate, a shorter period.

Employee benefits expenses

Employee benefits expenses include all costs related to employment including wages and salaries, fringe benefits tax, leave entitlements, redundancy payments, defined benefits superannuation plans, and defined contribution superannuation plans.

Financial asset

A financial asset is any asset that is:

- (a) cash;
- (b) an equity instrument of another equity;
- (c) a contractual or statutory right;
 - to receive cash or another financial asset from another entity; or
 - to exchange financial assets or financial liabilities with another entity under conditions that are potentially favourable to the entity; and
- (d) a contract that will or may be settled in the entity's own equity instruments and is:
 - a non-derivative for which the entity is or may be obliged to receive a variable number of the entity's own equity instruments; or
 - a derivative that will or may be settled other than by the exchange of a fixed amount of cash or another financial asset for a fixed number of the entity's own equity instruments.

Financial instrument

A financial instrument is any contract that gives rise to a financial asset of one entity and a financial liability or equity instrument of another entity. Financial assets or liabilities that are not contractual (such as statutory receivables or payables that arise as a result of statutory requirements imposed by governments) are not financial instruments.

Financial liability

A financial liability is any liability that is:

- (a) a contractual obligation:
 - (i) to deliver cash or another financial asset to another entity; or
 - (ii) to exchange financial assets or financial liabilities with another entity under conditions that are potentially unfavourable to the entity.
- (b) A contract that will or may be settled in the entity's own equity instruments and is:
 - (i) a non-derivative for which the entity is or may be obliged to deliver a variable number of the entity's own equity instruments; or
 - (ii) a derivative that will or may be settled other than by the exchange of a fixed amount of cash or another financial asset for a fixed number of the entity's own equity instruments. For this purpose, the entity's own equity instruments do not include instruments that are themselves contracts for the future receipt or delivery of the entity's own equity instruments.

Financial statements

A complete set of financial statements comprises:

- (a) a balance sheet as at the end of the period;
- (b) a comprehensive operating statement for the period;
- (c) a statement of changes in equity for the period;
- (d) a cash flow statement for the period;
- (e) notes, comprising a summary of significant accounting policies and other explanatory information;
- (f) comparative information in respect of the preceding period as specified in paragraphs 38 of AASB 101 *Presentation of Financial Statements*; and
- (g) a statement of financial position as at the beginning of the preceding period when an entity applies an accounting policy retrospectively or makes a retrospective restatement of items in its financial statements, or when it reclassifies items in its financial statements in accordance with paragraphs 41 of AASB 101.

Grants

Transactions in which one unit provides goods, services, assets (or extinguishes a liability) or labour to another unit without receiving approximately equal value in return. Grants can either be operating or capital in nature.

While grants to governments may result in the provision of some goods or services to the transferor, they do not give the transferor a claim to receive directly benefits of approximately equal value. For this reason, grants are referred to by the AASB as involuntary transfers and are termed non-reciprocal transfers. Receipt and sacrifice of approximately equal value may occur, but only by coincidence. For example, governments are not obliged to provide commensurate benefits, in the form of goods or services, to particular taxpayers in return for their taxes.

Grants can be paid as general purpose grants which refer to grants that are not subject to conditions regarding their use. Alternatively, they may be paid as specific purpose grants which are paid for a particular purpose and/or have conditions attached regarding their use.

Interest expense

Costs incurred in connection with the borrowing of funds Interest expenses include interest on bank overdrafts and short-term and long-term borrowings, amortisation of discounts or premiums relating to borrowings, interest component of finance leases repayments, and the increase in financial liabilities and non-employee provisions due to the unwinding of discounts to reflect the passage of time.

Net result

Net result is a measure of financial performance of the operations for the period. It is the net result of items of income, gains and expenses (including losses) recognised for the period, excluding those that are classified as 'other economic flows – other comprehensive income'.

Net result from transactions/net operating balance

Net result from transactions or net operating balance is a key fiscal aggregate and is income from transactions minus expenses from transactions. It is a summary measure of the ongoing sustainability of operations. It excludes gains and losses resulting from changes in price levels and other changes in the volume of assets. It is the component of the change in net worth that is due to transactions and can be attributed directly to government policies.

Net worth

Assets less liabilities, which is an economic measure of wealth.

Non-financial assets

Non-financial assets are all assets that are not 'financial assets'. It includes land, buildings, plant and equipment and intangible assets.

Other economic flows included in net result

Other economic flows included in net result are changes in the volume or value of an asset or liability that do not result from transactions. It includes:

- gains and losses from disposals, revaluations and impairments of non financial physical and intangible assets;
- fair value changes of financial instruments and agricultural assets; and
- depletion of natural assets (non produced) from their use or removal.

Payables

Includes short and long term trade debt and accounts payable, grants, taxes and interest payable.

Receivables

Includes amounts owing from government through appropriation receivable, short and long term trade credit and accounts receivable, accrued investment income, grants, taxes and interest receivable.

Supplies and services

Supplies and services generally represent cost of goods sold and the day-to-day running costs, including maintenance costs, incurred in the normal operations of the Inspectorate.

Transactions

Transactions are those economic flows that are considered to arise as a result of policy decisions, usually an interaction between two entities by mutual agreement. They also include flows within an entity such as depreciation where the owner is simultaneously acting as the owner of the depreciating asset and as the consumer of the service provided by the asset. Taxation is regarded as mutually agreed interactions between the government and taxpayers. Transactions can be in kind (e.g. assets provided/given free of charge or for nominal consideration) or where the final consideration is cash. In simple terms, transactions arise from the policy decisions of the government.

Appendix A – Disclosure Index

The Annual Report of the Commissioner for Privacy and Data Protection is prepared in accordance with all relevant Victorian legislation. This index has been prepared to facilitate identification of compliance with statutory disclosure requirements.

Legislation	Requirement	Page Reference
Ministerial Directions		
Report of Operations – FRD Guidance		
Charter and purpose		
FRD 22G	Manner of establishment and the relevant Ministers	Page 10–11
FRD 22G	Objectives, functions, powers and duties	Page 11
FRD 22G	Nature and range of services provided	Page 12–38
Management and structure		
FRD 22G	Organisational structure	Page 39
Financial and other information		
FRD 8D	Performance against output performance measures	Page 78
FRD 10A	Disclosure index	Page 75–76
FRD 12A	Disclosure of major contracts	Page 43
FRD 15C	Executive officer disclosures	Page 73
FRD 22G	Employment and conduct principles	Page 41
FRD 22G	Occupational health and safety policy	Page 41
FRD 22G	Summary of the financial results for the year	Page 44–74
FRD 22G	Application and operation of <i>Freedom of Information Act 1982</i>	Page 41
FRD 22G	Application and operation of the <i>Protected Disclosures Act 2012</i>	Page 43
FRD 22G	Details of consultancies over \$10 000	Page 42
FRD 22G	Details of consultancies under \$10 000	Page 42
FRD 22G	Statement of availability of other information	Page 43
FRD 24C	Reporting of office-based environmental impacts	Page 41
FRD 29A	Workforce Data disclosures	Page 40
FRD 22G	Disclosure of ICT expenditure	Page 43
SD 4.5.5.5	Attestation for compliance with <i>Ministerial Standing Directions 4.5.5</i>	Page 77
Financial statements required under Part 7 of the FMA		
SD4.2(a)	Statement of changes in equity	Page 51
SD4.2(b)	Operating statement	Page 49
SD4.2(b)	Balance sheet	Page 50
SD4.2(b)	Cash flow statement	Page 52

Legislation	Requirement	Page Reference
Other requirements under Standing Directions 4.2		
SD4.2(c)	Compliance with Australian accounting standards and other authoritative pronouncements	Page 53
SD4.2(c)	Compliance with Ministerial Directions	Page 53
SD4.2(d)	Rounding of amounts	Page 61
SD4.2(c)	Accountable officers' declaration	Page 48
Other disclosures required by FRDs in notes to the financial statements		
FRD21B	Disclosure of Responsible Persons, Executive Officers and other Personnel (Contractors with Significant Management Responsibilities) in the Financial Report	Page 73
FRD103E	Non-Financial Physical Assets	Page 58
FRD110	Cash Flow Statements	Page 72
FRD114A	Financial Instruments – General Government Entities and Public Non Financial Corporations	Page 57

Legislation

Commissioner for Privacy and Data Protection Act 2014

Freedom of Information Act 1982

Protected Disclosure Act 2012

Financial Management Act 1994

Audit Act 1994

Financial Statements

Appendix B — Attestation Complying with Standing Direction 4.5.5

I, David Watts, certify that the Office of the Commissioner for Privacy and Data Protection has complied with the Ministerial Standing Direction 4.5.5 – Risk Management Framework and Processes during 2015/16. The Office of the Commissioner for Privacy and Data Protection Audit and Finance Committee has verified this.

A handwritten signature in black ink, appearing to read 'David Watts'.

DAVID WATTS

Commissioner for Privacy and Data Protection
17 August 2016

Appendix C – Budget Paper 3

Budget Paper Number Three (BP3) Output Performance 2015-16

In 2014-15, the Office of the Commissioner for Privacy and Data Protection (CPDP) was required to report on legacy measures BP3 published prior to the creation of CPDP. 2015-16 is therefore the first year of reporting on CPDP performance measures as published in the 2015-16 budget.

Performance measures	Unit of measure	2015-16 actual	2015-16 target	Performance variation (%)	Result ¹
Quantity					
Law enforcement, data security and privacy reviews completed.	number	5	5	0	✓
Quality					
Client satisfaction with data security and privacy training provided.	per cent	99.0	90.0	+9.0	✓
<i>High levels of satisfaction by initial users of privacy training. Satisfaction levels are expected to move towards target with higher usage and following the introduction of data security training.</i>					
Timeliness					
Responses within 15 days to written enquiries relating to the legislated responsibilities of the Commissioner of Privacy and Data Protection.	per cent	98.0	90.0	+8.0	✓

The 2015-16 actual exceeded the target due to effective processes introduced to manage what was expected to be a challenging target in CPDP's first full year of operation. The number and complexity of enquiries is expected to increase as Victorian citizens and the VPS become aware of the provisions of CPDP legislation.

Note:

- Performance target not achieved – exceeds 5 per cent variance.

✓ Performance target achieved or exceeded. [A variance exceeding 5 per cent is a significant variance that requires an explanation, including internal or external factors that cause the variance].

TM Performance target not achieved – within 5 per cent variance;

Enquiries Line 1300 666 444
www.cdp.vic.gov.au

