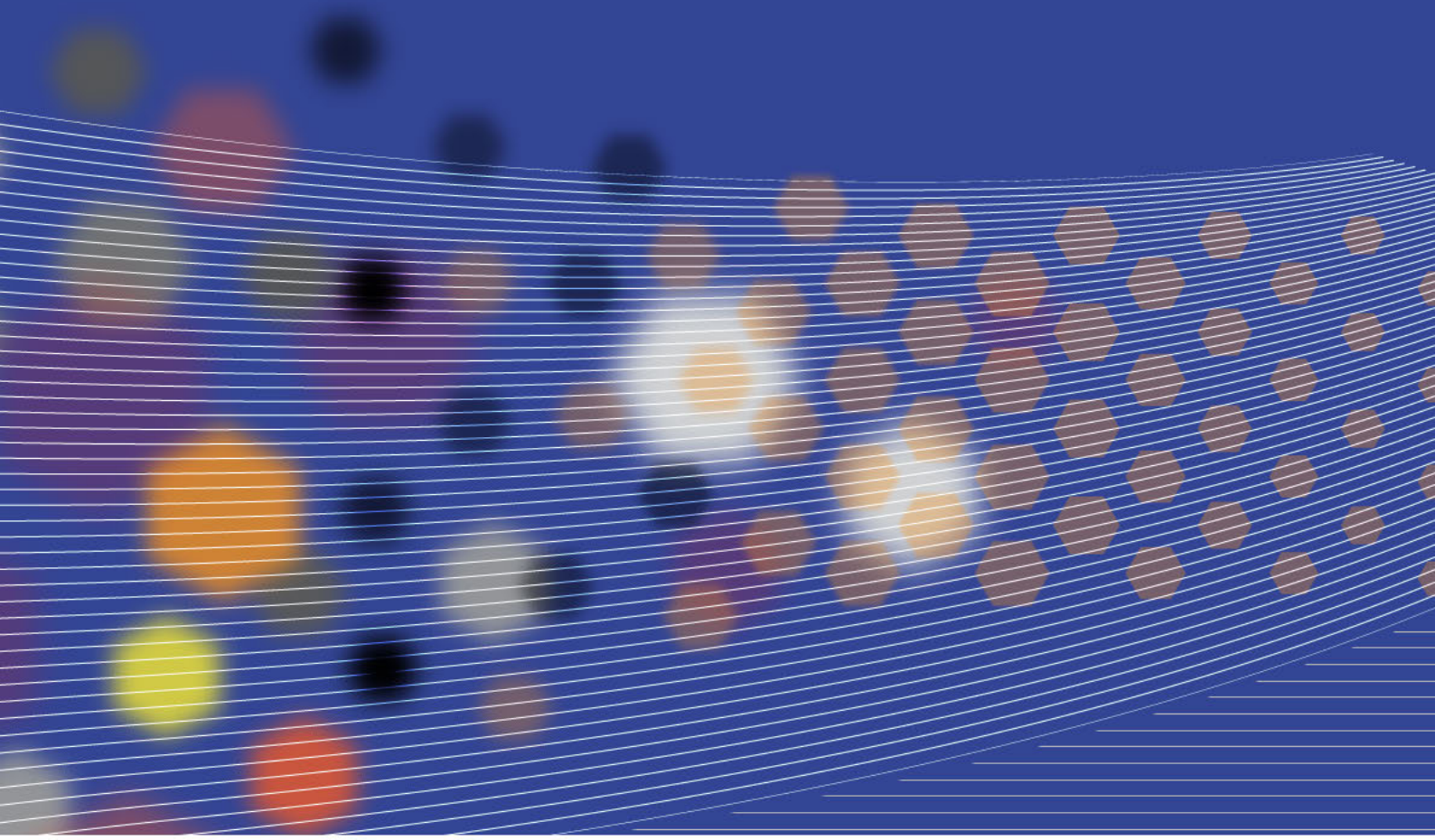
Commissioner for Privacy and Data Protection

Annual Report 2016–17



Commissioner for Privacy and Data Protection

VICTORIA State Government

Ordered to be printed
PP number 334, Session 2016-17

PDP 8574

Commissioner
for Privacy and
Data Protection

26 September 2017

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 2016-17 in accordance with Part 6 section 116 (1) of the *Privacy and Data Protection Act 2014*, for presentation to Parliament.

Yours sincerely

SVEN BLUEMMEL
Information Commissioner

Commissioner for Privacy and Data Protection
PO BOX 24014, MELBOURNE VIC 3001 T +61 3 8684 1660 W cpdp.vic.gov.au E enquiries@cpdp.vic.gov.au

Commissioner for Privacy and Data Protection

Annual Report 2016–17

Disclaimer

On 1 September 2017 the Office of the Victorian Information Commissioner (OVIC) replaced the Commissioner for Privacy and Data Protection (CPDP). This report reflects circumstances as at 30 June 2017 and is therefore written in the present tense in context.

The purpose and functions of the Privacy and Data Protection Act remain unchanged following the creation of OVIC.

Contents

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 It repealed the *Information Privacy Act 2000* and the *Commissioner for Law Enforcement Data Security Act 2005*, but combined those regulatory functions in the one piece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 *Privacy and Data Protection Act 2014* was amended by the *Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2016*. While a new office was created, Office of the Victorian Information Commissioner, the purpose and functions of the Privacy and Data Protection Act remain unchanged.

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 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:

- 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

The Operational Privacy and Assurance team (OPA) engages directly with regulated organisations and the general public. OPA supports and encourages good privacy practice, and when things go wrong, helps individuals to understand their rights and to access remedies.

Operational Privacy and Assurance does this by:

- responding to enquiries about privacy from the general public and from staff of regulated organisations
- working with both sides to conciliate privacy complaints
- advising regulated organisations on the management and remediation of privacy breaches when they occur
- examining the acts and practices of regulated organisations to assess their compliance with the Information Privacy Principles (IPPs).

Enquiries

CPDP operates a general privacy helpline and receives general privacy enquiries by email and post from members of the public and staff of regulated organisations. Responding effectively to general enquiries helps to grow the public understanding of the IPPs and supports public sector employees to handle personal information in a responsible and transparent way. CPDP's enquiries work also supports the broader work of the office by providing a valuable source of intelligence about the day to day issues faced by our stakeholders.

CPDP received 1551 enquiries during 2016–17. The vast majority of these were by phone (75%), with around a fifth received by email (21%), and the remainder being received by post (2%) or through the online complaint form on the CPDP website (2%). Of these:

- 41% related to matters that fall outside the Commissioner's jurisdiction. These enquiries are referred to the appropriate organisation for action — most commonly, 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).
- 42% involved questions about the application or interpretation of the *Privacy and Data Protection Act 2014* and the IPPs. Approximately two thirds of these come from members of the public, with the remainder from staff of public sector organisations.

  Questions from members of the public most commonly relate to concerns about specific acts or practices of organisations. In this context, CPDP officers provide general guidance about any relevant IPPs and how they may apply in the circumstances.

Additionally, where appropriate, we may refer the enquirer back to the privacy officer of the relevant organisation, engage with the relevant organisation on the enquirer's behalf, or assist the enquirer to make a formal complaint.

Questions from staff of public sector organisations most commonly involve matters about the interpretation of the IPPs in a given scenario. Callers may be privacy officers or information managers in their organisations, or may be concerned public sector employees with questions about information privacy. In both cases, CPDP officers help callers understand their obligations and apply good privacy practices.

- 15% were more general enquiries relating to CPDP, it's staff and services. These include requests for copies of CPDP publications, enquiries about training and media enquiries.
- 2% were organisations contacting CPDP to report a privacy breach.

Complaints

One of the Commissioner's functions under the *Privacy and Data Protection Act 2014* is to receive privacy complaints about organisations covered by the Act. The Commissioner's only function in relation to privacy complaints is to endeavour to resolve by conciliation the matters that give rise to the complaint. Where conciliation is inappropriate, or the Commissioner has grounds to decline to entertain a complaint, it may be dismissed and the complainant may have the matter referred to the Victorian Civil and Administrative Tribunal (VCAT) for hearing.

During the 2016–17 reporting period, CPDP handled 46 complaints (39 new complaints and 7 carried forward from 2015–16). This is a significant increase in complaints workload during the reporting period – compared to only 20 new complaints received in 2015–16.

CPDP finalised 24 complaints during the reporting period. Of these, the majority were declined to be entertained by the Commissioner (17) or considered inappropriate for conciliation (2). Three were conciliated successfully and two conciliated unsuccessfully. Where the Commissioner declined to entertain a complaint, the grounds most often relied on were that the act or practice complained of was not an interference with privacy, or that the respondent had dealt or was dealing adequately with the complaint.

Of the 21 complaints that were closed but not resolved by CPDP, 16 were referred to VCAT at the complainant's request.

Focusing on conciliation and resolution

In early 2017, CPDP noted that when responding to complaints, many organisations naturally concentrate on technical legal arguments about liability and fault. Of course, there is a place for these arguments. It is important when responding to a complaint, for organisations to seriously consider whether and to what extent they may have breached the IPPs. However, an undue focus on legal argument can displace more practical options for resolution, often to the detriment of both parties. As the Victorian Ombudsman observed in her April 2017 report *Apologies*, where someone has a legitimate grievance, remedies as simple as an apology can have powerful effect. In view of this, CPDP has taken steps towards refocusing complaints work on conciliation at all stages, including prior to a formal complaint being lodged, and has began a review of it's internal templates and guidance to this end.

Complaint handling process improvements

In 2015–16, CPDP completed a review of its privacy complaints handling process. Following on from this work, CPDP has implemented a number of process improvements aimed at streamlining the complaints handling process. These include moving to fully electronic file management and simplifying the internal approval processes associated with the management of complaints.

VCAT Monitoring

The Commissioner is empowered to intervene or join privacy proceedings before VCAT at his discretion, or with leave from the Tribunal. The Commissioner may exercise this power where a significant question of law is raised, where proceedings may have significant implications for the ongoing application, interpretation, implementation and/or operation of the Privacy and Data Protection Act, and/or where participation is otherwise in the public interest. In order to support the Commissioner in his exercise of this function, OPA monitors and assesses all current privacy proceedings before VCAT.

Privacy 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 respond to enquiries and complaints and demonstrates public sector commitment to transparent and accountable privacy practices.

When responding to privacy breach notifications, we vary our approach based on the nature and severity of the breach. We put the affected individuals first, and focus on assisting the organisation to contain the breach, reduce the impact of the breach on affected individuals and take steps to mitigate the risk of similar incidents in the future.

The number of breach notifications received by the Commissioner has increased significantly over the last three years, from 13 in 2014–15, to 27 in 2015–16, to 35 in the current reporting period. This trend reflects a broadening appreciation among regulated organisations of the importance of actively managing privacy incidents and the value in proactively engaging with our Office.

Almost two thirds (65%) of all reported breaches during 2016–17 were the result of human error. Most commonly, these breaches involved:

- misaddressed emails (22% of all reported breaches)
- misaddressed physical mail (14%)
- information accidentally published online (11%)
- physical documents, USBs or laptops being lost or left in public places (8%)

A quarter (25%) of reported breaches were the result of misconduct or criminal activity. These breaches can be divided into three broad categories:

- incidental breaches resulting from criminal activity that does not appear to be targeted at accessing or misusing personal information (14% of all reported breaches)
- breaches involving 'insider threats' such as employee theft of government data (8%)
- breaches involving third party hacking, social engineering or other external attacks (3%)

DHHS Reviews

In 2016, CPDP identified an increase in privacy and data security reports and complaints involving the Department of Health and Human Services (DHHS). At the same time, we saw a series of confronting media reports emerge highlighting privacy and security deficits, particularly in relation to the Department's home based care and family violence operations. These reports were followed by an independent review of child protection privacy incidents, which raised significant concerns about the number of reported privacy breaches over the last five years.

In response, CPDP announced two major reviews of the Department of Health and Human Services (DHHS). The first review looked at information governance across the Department as a whole, while the second focused specifically on information security practices and procedures in relation to the Department's home based care and family violence operations. Both reviews were finalised in January 2017.

The *Review of information governance in the Department of Health and Human Services (DHHS)* identified a number of shprtcomings in the Department's information governance arrangements and made recommendations about how they should be addressed. The recommendations focus on the management of contracted service providers, staff training, information asset management and incident reporting.

The *Review of information security practices and procedures in relation to the home based care and family violence operations of the Department of Health and Human Services (DHHS)* identified similar issues at the program level. Recommendations were made covering training for frontline workers, document classification, contracted service provides' privacy and security arrangements, and enhancing stakeholder relationships.

The reviews benefitted from an open and collaborative approach on both sides, and the Department of Health and Human Services is already well advanced in its implementation of the recommendations.

Strategic Privacy

Privacy Policy – Practical Privacy and Engagement

The Strategic Privacy team within CPDP has primary responsibility for leading the office's privacy policy work. Over the past year the team has made a concerted effort to provide CPDP's stakeholders with a more practical approach to implementing privacy. This has involved preparing user-friendly tools and resources that target commonly experienced privacy issues, and enhancing the level of engagement with practitioners to better understand how CPDP can support them in managing the privacy challenges they face. Some of the initiatives that the Strategic Privacy team has launched during the past 12 months to facilitate better engagement include a Privacy Blog and quarterly privacy forums that are open to the public, at which topical privacy issues are presented and debated. The forums attract a healthy audience attending both in person and via online streams.

The Strategic Privacy team also continues to increase its engagement with counterparts in other Australian states and internationally. In particular, the team actively participates in networks of privacy regulators, including the Asia Pacific Privacy Authorities (APPA), the Global Privacy Enforcement Network (GPEN) and the Common Thread Network. Some of the international activities that the Strategic Privacy team has been involved in include Privacy Awareness Week, attendance at biannual APPA forums, participation in the annual GPEN Sweep, and taking part in monthly GPEN teleconferences. These forums allow CPDP a platform to express the Victorian perspective on privacy, and have provided an opportunity to shape international thinking on important privacy issues.

Since CPDP was established the landscape of privacy in Victoria has shifted dramatically. In particular, there is a more prevalent awareness amongst the Victorian public sector of information privacy, and an increased understanding of why privacy is important to Victorians. This shift has been demonstrated through an increase in the number of agencies that proactively engage with CPDP when implementing new programs that involve personal information, showing that they are turning their attention to privacy impacts early on in the process.

Privacy by Design

The term 'Privacy by Design' has become part of the vocabulary of privacy advocates and practitioners across the Victorian public sector, and organisations are continuing to engage with this concept by taking proactive steps to identify and mitigate privacy risks. One of these steps is conducting privacy impact assessments (PIAs). The Strategic Privacy team has been asked to provide feedback on 15 PIAs completed by public sector organisations, more than doubling the number received in the previous reporting period. This encouraging number highlights that CPDP has made significant progress in promoting Privacy by Design, and that organisations are finding utility in conducting these assessments. Many of the PIAs reviewed share similar themes, including transition to online services for citizens and the implementation of new technologies.

In addition to external PIAs, CPDP has also conducted a number of PIAs on internal projects and tools, many of them aimed at facilitating better engagement with stakeholders. Examples include an online tool to manage guest registrations for events and the CPDP Privacy Blog.

Outsourcing

A key theme for the Victorian public sector over the past 12 months has been establishing and managing relationships with contracted service providers (CSPs) in respect of privacy and data security requirements. We have seen a number of high-profile examples in the media of privacy breaches involving personal information held by CSPs, many of which have involved the accidental or inadvertent disclosure of personal information to unauthorised parties. One particular incident prompted the Commissioner to launch a review into the governance and information handling practices of the involved parties (see the Operational Privacy and Assurance section of this report).

In response to the reviews findings, CPDP developed new guidance on outsourcing in the Victorian public sector. The guidance contains two documents – a checklist and accompanying explanatory guide – that prompt organisations to think about the privacy and data security impacts of an outsourcing arrangement before they engage a CSP, during the performance of a contract, and once a contract has been fulfilled.

In addition to the new guidance, outsourcing was the subject of a workshop delivered during Privacy Awareness Week (PAW) in May. Tying in with this year's theme, *Trust and Transparency*, PAW was the opportune time for CPDP to offer training to Victorian public sector staff on how to ensure due diligence in respect of privacy and data security when engaging CSPs. The guidance and workshop were both well received, and CPDP anticipates these resources will assist organisations to better understand the potential privacy issues associated with outsourcing.

Submissions

The Strategic Privacy team regularly makes submissions to consultations that have an impact on privacy. In some cases, CPDP is directly invited to comment on an initiative, while in others the Strategic Privacy team identifies relevant areas of law reform or policy that are open for public consultation. In the past financial year CPDP has made nine submissions to various inquiries.

Some of the consultations that CPDP has made submissions in response to include:

- the National Transport Commission's work into automated vehicle trials
- the Productivity Commission's Data Availability and Use inquiry
- a review of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*
- a civil penalty regime for non-consensual sharing of intimate images.

CPDP's response to each of these consultations is publicly available on the CPDP website.

Practical Privacy for Victoria

Social media

The Strategic Privacy team identified social media as an area in which the Victorian public sector could benefit from further guidance. All organisations are starting to make use of social media in some form to enhance their business practices and engage with stakeholders, but in some cases, there may be privacy implications that need to be managed. CPDP produced a set of FAQs in response to common questions received on this topic, and also held a public forum on social media and privacy. A recap of the forum and the issues discussed has been published on the Privacy Blog.

The Strategic Privacy team also produced an information sheet on the use of instant messenger within organisations, outlining some of the issues that should be considered, and the privacy risks that should be addressed, before using these tools.

Surveillance

CPDP often receives enquiries from members of the public as well as public sector organisations in relation to using surveillance devices to monitor individuals and groups, most often closed-circuit television (CCTV). In response, the Strategic Privacy team produced guidelines on the use of surveillance technologies in the Victorian public sector, which contained a set of principles that organisations should consider when deciding to undertake surveillance activities. Surveillance and privacy was also the topic of discussion at the public forum held during Privacy Awareness Week 2017, at which we heard from academics as well as practitioners who use surveillance as part of their work.

Workplace privacy

The workplace raises a number of privacy issues for both employers and employees. The Strategic Privacy team prepared an information sheet to consolidate many of the issues that CPDP receives enquiries about, including the responsibilities that employers have during the recruitment stage to protect applicants' privacy, and the rights of employees to expect a certain level of privacy when at work.

Reasonable steps to protecting personal information

Under the *Privacy and Data Protection Act 2014* organisations must take reasonable steps to protect the personal information they hold. Following the issuing of the Victorian Protective Data Security Standards (VPDSS), the Strategic Privacy team produced guidelines for organisations on what reasonable security of personal information means, drawing from the VPDSS. This document provides practical steps for organisations to consider when deciding how to protect the information they hold.

Flexibility mechanisms

In July 2016, the Commissioner approved the first certification under the *Privacy and Data Protection Act 2014*. An application was submitted by the Victorian Auditor-General's Office (VAGO) requesting that the Commissioner certify that the steps they take to provide notice to individuals that their personal information has been collected during the course of audits, was sufficient in meeting the intent of Information Privacy Principle 1.5. The Commissioner was of the opinion that the steps VAGO takes to provide notice are 'reasonable' given the circumstances. The Commissioner's certificate and response to the request are available on the CPDP website.

CPDP continues to consult with organisations who wish to enquire about applying for a flexibility mechanism.

Data Protection

The Victorian Protective Data Security Framework (VPDSF) was issued in June 2016, meeting a statutory obligation established by the Privacy and Data Protection Act 2014 (PDPA). The VPDSF is binding on all applicable Victorian public-sector agencies and bodies.

The Framework consists of:

- Victorian Protective Data Security Standards (VPDSS)
- Assurance model
- Supplementary security guides and supporting materials.

The Victorian Protective Data Security Standards (VPDSS)

The **Victorian Protective Data Security Standards** were issued under the Framework at the beginning of the current reporting period.

The Standards establish 18 high level mandatory requirements to protect public sector data and provide for governance across the four domains of information, personnel, ICT and physical security.

Each standard is supported by four protocols. This follows the continuous improvement process of plan, do, check, and act (see Guiding Principles for details). This enables 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 government environment
- focus on the security of information
- identify information security and ICT security as individual yet equally important security domains
- require organisations to ensure contracted service providers with direct or indirect access to information adhere to the standards.

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

Supplementary security guides and supporting material

Considerable effort was given during the year to producing supplementary security guides and supporting materials for the Standards using internal CPDP resources.

In particular the Commissioner published:

- **VPDSF Information Security Management Collection.** This collection is the starting point in helping organisations evaluate the relationship between its information and the way in which it supports the business needs of the organisation.

  The Information Security Management Collection covers:

  Chapter 1 – Identifying and Managing Information Assets

  Chapter 2 – Understanding Information Value

  Chapter 3 – Protective Markings

  The collection also includes the following supporting resources for each chapter:

  Chapter 1 – Appendix A – Sample questions and example information assets

  Chapter 1 – Appendix B – Sample Information Asset Register (IAR) template

  Chapter 1 – Appendix C – Information Asset considerations

  Chapter 1 – Appendix D – Suggested Information Management roles and responsibilities

  Chapter 2 – Appendix A – Stages of the information value assessment process

  Chapter 2 – Appendix B – VPDSF Business Impact Level (BIL) Table

  Chapter 2 – Appendix C – BIL Mobile App

  Chapter 3 – Appendix A – Relationship between protective markings

  Chapter 3 – Appendix B – Common protective markings employed by each State and Territory

  Chapter 3 – Appendix C – Ready reckoner: How to select an appropriate protective marking

- **Assurance Collection.** The Assurance Collection supports organisation's VPDSF reporting obligations under Part 4 of the Privacy and Data Protection Act (2014). The Assurance model seeks to ensure that the security capability and maturity levels in the Victorian public sector are as reported by organisations. CPDP will in turn analyse and report on organisations' security capability and maturity in its reporting back to government. The activities set out in this collection assist organisations to identify, analyse and evaluate their security risks more effectively, and then manage these through the use of existing risk management frameworks or by referencing established risk management material.

The Assurance Collection covers:

Chapter 1 – Protective Data Security Risk Profile Assessment

Chapter 2 – Measuring and reporting implementation of the VPDSS

Chapter 3 – Protective Data Security Plan

The collection also includes the following supporting resources for each chapter:

Chapter 1 – Appendix A – Example Security Risk Profile Assessment Template

Chapter 1 – Appendix B – Summary of SRPA Actions

Chapter 2 – Appendix A – VPDSS Self-assessment Template

Chapter 2 – Appendix B – Summary of VPDSS Self-assessment Actions

Chapter 3 – Appendix A – Protective Data Security Plan (PDSP) Template

Chapter 3 – Appendix B – Summary of PDSP Actions

The Monitoring and Assurance System (MAS)

By July 2018 applicable Victorian government organisations are required under the PDPA to submit Protective Data Security Plans (PDSP) to CPDP and a self-assessment compliance position.

Funding has been provided by government for the implementation of software to enable the assurance model and CPDP to meet its on-going function of monitoring and assurance.

Software is required to receive the self-assessments, PDSPs agency attestations, and also to give CPDP the capacity to run data analytics across them in order to identify the information security risk profile of the Victorian public sector as a whole. The software will further enable CPDP to identify threats to Victorian public sector data and identify vulnerabilities across the physical and digital storage, processing and handling of public sector data. These vulnerabilities are those that could be exploited to gain access to public sector data, corrupt it of or render it unavailable.

The software will be owned by CPDP, but will also be used by all contributing public sector agencies to identify and manage their information security risks. It will enable agencies to track their developing information security maturity and enable CPDP to track the overall information security risk maturity of the Victorian public sector.

This approach is expected to minimise the reporting burden on Victorian public sector agencies by using a tool that can track risk and control frameworks, for example NIST Cyber Security Framework, Enterprise Solutions Branch Statement of Directions, VPDSS, Australian Government Protective Security Policy Framework (PSPF), ISO27001, Payment Card Industry Data Security Standards (PCI-DSS). The tool will collect the data once and then have the capability to extract the data in various ways across the public sector. This will help where there are information sharing agreements locally and with other states and territories. As such this initiative supports the demand for improved information sharing across Victorian public sector organisations, with contracted service providers and across jurisdictions.

Funding for the procurement, implementation and on-going maintenance of the software solution, together with additional staff and MAS specific training modules was provided late in the reporting period.

At the time of writing a procurement/ implementation project is being commenced.

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 broader framework of protective data security, explicitly stating the Commissioner's jurisdiction over Victoria Police and the 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 had previously developed and issued the Crime Statistics Data Security Standards (CSDSS). The CSDSS describe the standards, objectives, protocols and best practice implementation guidance required to protect information received, held and used by CSA.

In July 2016 the Commissioner issued the Victorian Protective Data Security Standards (VPDSS). The VPDSS are applicable to all Victorian Public Sector Agencies. In November 2016 the Commissioner revoked the CSDSS and applied the VPDSS to the Crime Staistics Agency. This enabled the CSA to align with Whole of Victorian Government information security obligations.

While the VPDSS requires the first round of public sector assurance reporting to be completed by August 2018 (covering FY 2017-18), the CSA took advantage of VPDSS assurance processes and documentation to deliver their 2016-17 annual assurance report to CPDP.

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 VPDSS and that adequate controls are in place to mitigate identified risks to crime statistics data.

Victoria Police

Transition to the Victorian Protective Data Security Standards (VPDSS)

In early 2017 the Commissioner advised Victoria Police of his intention to revoke the Standards for Law Enforcement Data Security and transition the organisation as of 1 July 2017 to the Victorian Protective Data Security Standards, thus bringing Victoria Police in line with the rest of the Victorian Public Sector.

The VPDSS are less prescriptive than the SLEDS, but harmonised with them. The VPDSS imposes no further obligations on Victoria Police, but changes the focus from straight compliance to a risk management approach.

Implementation of Recommendations

Implementation Working Group (IWG)

The joint Victoria Police and CPDP IWG continued to meet and progress outstanding recommendations throughout 2016-17.

Victoria Police implemented eleven outstanding recommendations in 2016-17 and provided a further 9 recommendation responses for consideration by CPDP. This is a significant achievement given that most outstanding recommendations are IT/System specific and often require business case funding.

In 2016-17, five new recommendations were issued by CPDP under the *Review of the Victoria Police Security Incident Management Framework and Practices*.

The history of implementation and the current implementation status of recommendations at 30 June 2017 is shown in the following table.

Status	Pre IWG	30/6/12	30/6/13	30/6/14	30/6/15	30/6/16	30/06/17
Implemented	41	71	132	164	166	172	183
Not Fully Implemented	110	54	41	25	24	24	25
Not Implemented	62	56	41	23	30	24	16
Not Implemented – Risk Managed [1]	-	-	-	-	-	0	0
Withdrawn	0	32	39	41	41	41	42
Total Recommendations	213	213	253	253	261	261	266
Total Outstanding	172	110	82	48	54	48	41
% of active recommendations implemented	19%	39%	62%	77%	75%	78%	82%

1 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 of address similar or related issued. Any future recommendations will be reviewed on their own merits.
In 2016-17, no outstanding recommendations were finalised as *Not implemented – Risk Managed*.

Breach Reporting – Security Incident Register

The Security Incident Registry (SIR) is the central repository within Victoria Police for the reporting, recording, recovery and post-incident analysis of information security incidents and events.

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 previously reported incidents, including new information, changes to impact assessment or status progress, including those marked as completed.

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

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 2015-16, the SIR recorded 453 information security incidents. In 2016/17 the SIR dealt with 547 information security incidents – a 21% increase from the previous financial year and a 65% increase from 2014-15 financial year (332). This increase highlights an improving organisational maturity around information security incident identification and reporting, and enhanced information capture by the SIR. This should be seen as a positive example of improved security incident management by Victoria Police.

At 30 June 2017, 496 incidents were marked complete, including 25 being found to constitute no information security incident upon file completion. 51 incidents remain in progress (including those reported to the SIR by PSC - see the 'PSC reporting to the SIR' section for further discussion).

Figure 2. Information Security Incidents – By Type

Type	Count
Lost or stolen police certificates of identity	258
Data Spill	52
Unauthorised release or disclosure of information	41
Theft or loss of asset	38
Abuse of privilege	27
Other Event	23
No Incident	20
Unauthorised Access	18
Threat to facility	16
Failure of Process	14
Configuration Error	12
Password Confidentiality	5
Unauthorised changes to information, applications, system or hardware	4
Unprofessional Conduct	4
Access Controls	3
Stolen VicPol Credentials	3
Malware Infection	2
Manipulation of controls	2
Suspicious system behaviour or failure	2
Denial of Service	1
Fraudulent Activity	1
Unauthorised surveillance devices	1

Figure 3. Potential or actual consequence assessment (as at 30 June 2017)

Incident Assessment	Count
MAJOR	1 [2]
MODERATE	35
MINOR	126
INSIGNIFICANT	352
No Incident	25
Unable to assess	8

2 While classified as a major incident, investigation showed that the incident could not be attributed to a Victoria Police employee

The Security Incident Registry risk-rates all protective security incidents in order to attribute a risk priority. This assessment process incorporates specific protective security incident consequences and, importantly, aligns with Victoria Police's organisational risk identification and assessment processes established by the Chief Risk Officer.

This risk management approach allows Victoria Police to implement effective control, or treatment, strategies to reduce potential or actual consequences arising from identified risks.

The Escalated Reporting Protocol established between CPDP and Victoria Police outlines key thresholds and requirements that are triggers to reporting to CPDP[3].

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. 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.

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

- the context of the incident
- 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 2017, 121 information security incidents had been reported to CPDP under the obligations set out in the escalated reporting protocol.

3 For instance, incidents assessed by Victoria Police as having a catastrophic or critical consequence, Major, or Moderate are directly reported to the Commissioner by verbal and written briefings. Those assessed as Minor or Insignificant are reported via weekly reports.

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 by members of Victoria Police, including breaches of information security.

ROCSID Statistics [4]

CPDP extracted data via a standardised report function executed within the ROCSID database.

The report returned 173 incidents / allegations containing an information security element recorded in ROCSID in 2016-17.[5]

- PSC determined 27 allegations of information security breaches to be true via formal investigation.
- 39 allegations are yet to be finalised.
- 51 allegations were dealt with by management intervention. Allegations resulting in management intervention focus on service delivery complaints, or employee performance management and are not subject to a formal investigation by PSC.
- 56 allegations were finalised (Allegation determination: not substantiated, unable to determine, no complaint, unfounded, filed for intelligence purposes)

4 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.

5 Report generated August 2017. 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.

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 2016-17 the SIR recorded 81 information security incidents reported to them by PSC. As at 30 June 2017, 42 investigations had been reported by PSC as being completed, with 39 incidents still under investigation.

Review of Victoria Police Security Incident Management framework and practices

In January 2017, CPDP finalised a review of the Victoria Police Security Incident Management Framework for the protection of law enforcement data, including a critical assessment of organisational security incident management practices.

The review aimed to determine the extent to which Victoria Police has implemented an effective Security Incident Management (SIM) framework, and practices. Embodied in the protective data security standards (SLEDS, and now within the VPDSS) are two key objectives of an effective SIM framework:

- 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.

The review established a consistent set of factors to be considered by Victoria Police when determining its approach in managing security incidents – a framework for best practice security incident management.

The review recommended that Victoria Police adopt and implement this Framework in order that the Organisation's security incident management and practices align with those of the wider Victorian Public Sector as implementation of the VPDSS takes place.

CPDP and Victoria Police identified and agreed upon a set of high-level findings fundamental to improving security incident management and practices within Victoria Police.

CPDP recommended that Victoria Police review, validate and update security incident management policies ensuring they are simplified, integrated and communicated to all stakeholders.

The review emphasised the importance of a strong, centralised approach to information security awareness training to ensure consistency in content and delivery. Review participants commonly considered that lack of organisational awareness, rather than cultural reluctance to report, is the main barrier to more effective incident identification and reporting. Victoria Police should continue to actively promote a culture of incident reporting.

The review also stressed the need for Victoria Police to strengthen the link between security incidents and actual or potential risk. The review identified a separation and isolation of organisational risk assessment, governance, management, and capacity across various roles and functions responsible for managing security incidents. Work is currently being undertaken by Victoria Police to build a shared understanding of security risks and to align and integrate security incident management and practice with the organisational risk management framework.

The security incident management environment can be a complex, and often changing, landscape. Sound governance involves, in part, clear direction and the assignment and acknowledgement of responsibilities in security incident management and practice. The review underlined that Victoria Police needs to define, build, and maintain, a capability around security incident management roles and responsibilities. This includes understanding the functions, activities, objectives, expectations and accountabilities of stakeholders engaged within the Victoria Police security incident management landscape.

Survey of Victoria Police Members

Findings of the longitudinal (2012-2016) survey into Victoria Police's information security culture were reported in the Commissioner's annual report for the 2015-16 year. The survey has now finished and been passed to Victoria Police for any future survey waves.

'*BlueConnect*' Project (formerly 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-focussed in 2016, the project is now titled the *BlueConnect* program and includes three main technology-enabled programs being:

1. Mobile technology – delivering handheld mobile devices to frontline police
2. Body-Worn Cameras – audio and visual recording devices for front-line members
3. Intelligence capability – a new system to provide Victoria Police with enhanced intelligence collection and analytics

Victoria Police have kept CPDP briefed on progress across these important projects.

CPDP continues to closely monitor national and international trends in these emerging technologies, their potential impact (both positive and negative) both for policing and for the community, and the implications for privacy and data security. The Victoria Police Project team recognises that designing and building strong protective data security and privacy principles into the project from conception will be a key driver of organisational change management (including training, awareness, policy and processes).

Stakeholder Engagement

The Commissioner for Privacy and Data Protection conducts a broad range of activities to promote understanding of privacy and data protection issues, notably the Information Privacy Principles and the Victorian Protective Data Security Framework.

Networks

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) 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. The YAG is made up of approximately 10 members aged between 15 and 19, and meets four times per year.

During the reporting period, members of the group worked together to formalise group processes through the creation of a YAG charter. Members also produced content for the Privacy Blog and conducted an interview with the Foundation for Young Australians for a collaborative article *What a lot of people don't know about their privacy online*. The YAG also designed, prepared and ran a public workshop during Privacy Awareness Week 2017 called *Privacy: Not dead, just different*, that facilitated dialogue between different demographics on various understandings of privacy, in particular privacy for young people.

Inter-agency Privacy Officers' Forum

The Inter-agency privacy Officers' Forum was established in 2015 to bring together privacy officers from each of the Victorian government departments, key agencies, and staff from CPDP's Strategic Privacy and Operational Privacy and Assurance teams. The forum provides a useful opportunity for colleagues to share ideas and resources, discuss common privacy issues and learn from each other's experiences. Meetings are held quarterly and all members are invited to contribute to the agenda.

Privacy Awareness Week

An initiative of the Asia Pacific Privacy Authorities (APPA), Privacy Awareness Week is held each year in May to promote an awareness of the importance of privacy. The theme for this year was *Trust and Transparency* and CPDP held a number of events throughout the week of 8 – 12 May, including privacy training, a workshop on outsourcing and two public forums. For the first time CPDP also ran a creativity contest and asked the public to submit their interpretation of privacy in a creative format. Entries received included artwork, songs, poems, and photographs. The competition was won by a high school student who submitted an original drawing of what privacy means to her.

Asia Pacific Privacy Authorities

CPDP is a member of the Asia Pacific Privacy Authorities (APPA) forum, which brings together privacy regulators from around the Asia Pacific to exchange ideas and learn from the experiences of other jurisdictions. APPA meetings are held biannually and the Assistant Commissioner Strategic Privacy attended the 45th meeting in Singapore in July 2016, and the 46th meeting in Manzanillo, Mexico in December 2016. CPDP also actively participates in contributing to surveys and other consultations run by the APPA Secretariat throughout the year.

Global Privacy Enforcement Network

CPDP is an active participant in the Global Privacy Enforcement Network (GPEN), which is a network of privacy regulators from around the world that work to foster cross-border cooperation, particularly in enforcement. CPDP participates in the monthly teleconferences organised by GPEN, at which speakers present on topical privacy issues, and is on the GPEN Pacific Program Committee, which assists to identify speakers and discussion topics for the monthly calls.

CPDP also participates in the annual GPEN Sweep, the theme for which was 'User controls over personal information' in 2017. CPDP examined the privacy policies and collection notices of Victoria's universities and TAFEs to determine how well they communicate their information handling practices to prospective students upon applying for study at the institution. CPDP intends to produce its findings from the Sweep in late 2017.

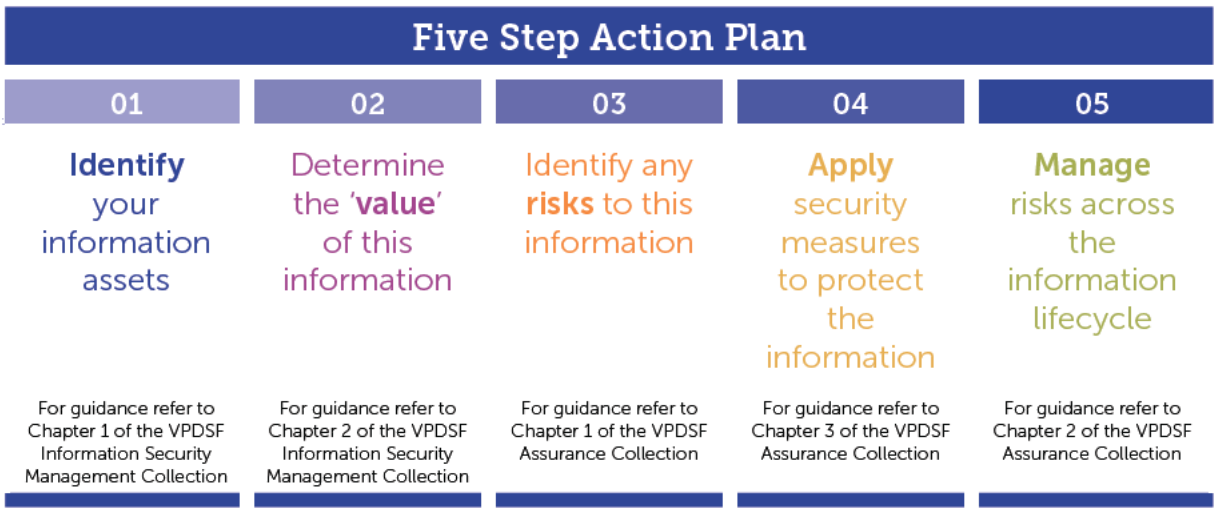
Common Thread Network

The Common Thread Network (CTN) was established in 2014 to facilitate a dialogue between privacy and data protection regulators within the Commonwealth. The aim of the CTN is to encourage governments that have not yet enacted privacy laws, to do so, and to promote good privacy practices in jurisdictions with relatively new privacy laws. CPDP participates in the CTN teleconferences, which are held every two to three months.

Victorian Information Security Network (VISN)

The Data Protection Branch hosted two inaugural forums in Melbourne and visited Victorian regional areas comprising Ballarat, Warrnambool, Geelong and Bairnsdale).

Attendees to these forums were provided a high-level briefing on the Victorian Protective Data Security Framework (VPDSF), including an overview of what the framework and standards mean for both individuals and their organisation. The Data Protection Team also presented a new five-step action plan.



Throughout the forums the audience was encouraged to ask questions and participate in polls. A new tool was trialled during the Melbourne sessions, providing attendees an opportunity to digitally engage and ask questions.

A high-level summary of responses from audience members who used this tool were provided in the VPS and PARTNERS infographics.

Overall, CPDP had a very positive response and this has helped us shape future forums.

State and Territory Security Representatives Meeting

The State and Territory security representatives meeting is a biannual meeting hosted in different locations in Australia to discuss government information security matters.

CPDP hosted the meeting of representatives in Melbourne in November 2016 and the Commonwealth Attorney-General's Department hosted the meeting in Canberra in May 2017. The meetings were well attended including representatives from New Zealand government with collaboration on security matters covering:

- information security
- personnel security
- physical security
- Federal government updates
- reporting, monitoring and assurance
- training, outreach and awareness

Digital tools for stakeholder engagement

To effectively engage with a broad range of stakeholders in a modern and accessible way, CPDP has shifted much of its engagement strategy toward a digital format. This enables CPDP to extend its reach and produce content that is readily accessible, practical and user-friendly.

Training

Online training modules

In March 2016 CPDP launched its *Introduction to privacy in the Victorian public sector* online training course. Now in its second year of existence, the training module continues to be popular, with 614 users completing the course in the first quarter of 2017. The interactive activity-based training provides public sector staff with an overview of their privacy obligations under the *Privacy and Data Protection Act 2014*. A downloadable version of the training has also been developed for organisations wishing to deliver their own in-house training.

CPDP has also started the development of an online training module that will serve as an introduction to data protection in the Victorian public sector.

Tools to enhance delivery of in-person training

To increase the efficacy of in-person training and events, CPDP uses Sli.do and Prezi to enhance the experience of stakeholders. Sli.do and Prezi are both web based applications designed to increase engagement when delivering face-to-face presentations. CPDP uses Sli.do to facilitate audience interaction through their personal devices. Sli.do allows users to participate in live polls, and post questions and comments to the presenters. CPDP also uses Prezi to produce presentation content that has been found to be more engaging than standard presenting tools. CPDP has received

positive feedback on the use of both tools regarding the level of audience interaction, attention, and the ability to visualise content- more clearly.

Content delivery and online tools

Information Sharing Interactive PDF

To complement the *Guidelines for sharing personal information*, CPDP developed a tool in the form of an interactive PDF to assist Victorian public sector organisations make decisions about whether or not it is appropriate to share personal information in a given context. It was identified that many public sector employees were more likely to engage with an interactive step-by-step process as offered by this tool, than to consult a lengthy guidance document in the first instance.

Videos

CPDP has two informational videos available online relating to topics that receive a high number of enquiries to the office. The first, *How to make a privacy complaint*, is targeted at the general public and is designed to clarify the process of making a complaint to CPDP. The second, *What is security?,* is for public sector organisations covered by Part 4 of the *Privacy and Data Protection Act 2014* and outlines key elements of protective data security and the Victorian Protective Data Security Framework.

CPDP App

Launched in 2016, the CPDP App acts as a digital reference library of published material. All of the resources available on the CPDP website are reflected in the app in order to increase the accessibility of guidance materials for the public and public sector employees.

Business Impact Level (BIL) App

The Business Impact Level (BIL) App is designed specifically to assist Victorian public sector employees to determine which protective marking is most appropriate for the data they are handling. The app asks a number of questions to determine the BIL of the material and prompts the user to the most appropriate protective marking. As many employees are short on time and resources and may not have an in-depth understanding of protective data security, the app was designed to make the process as simple as possible.

Social media and communication

Twitter

CPDP uses Twitter to engage with various stakeholders in a number of ways: to launch and promote new and existing material or other content such as upcoming events and training sessions, to engage with groups or organisations associated with the privacy and data protection online community, and to engage with the public on topical issues pertaining to privacy and data protection. Since revitalising the CPDP Twitter account in 2016, @CPDPVICAU has steadily increased its followers, with a 74% increase over the past financial year.

Periscope

The Strategic Privacy team holds quarterly public forums on current privacy issues. To maximise participation, CPDP utilises Periscope – a web-based application that allows users to stream content from their personal device – to broadcast the forums live online. A recording of the event is also published on CPDP's Periscope channel for audiences to view at a later time. The Strategic Privacy team has found that there has been widespread support for streaming forums online, as many interested parties from around Victoria and interstate are able to engage with the content despite not being physically present.

Privacy Blog

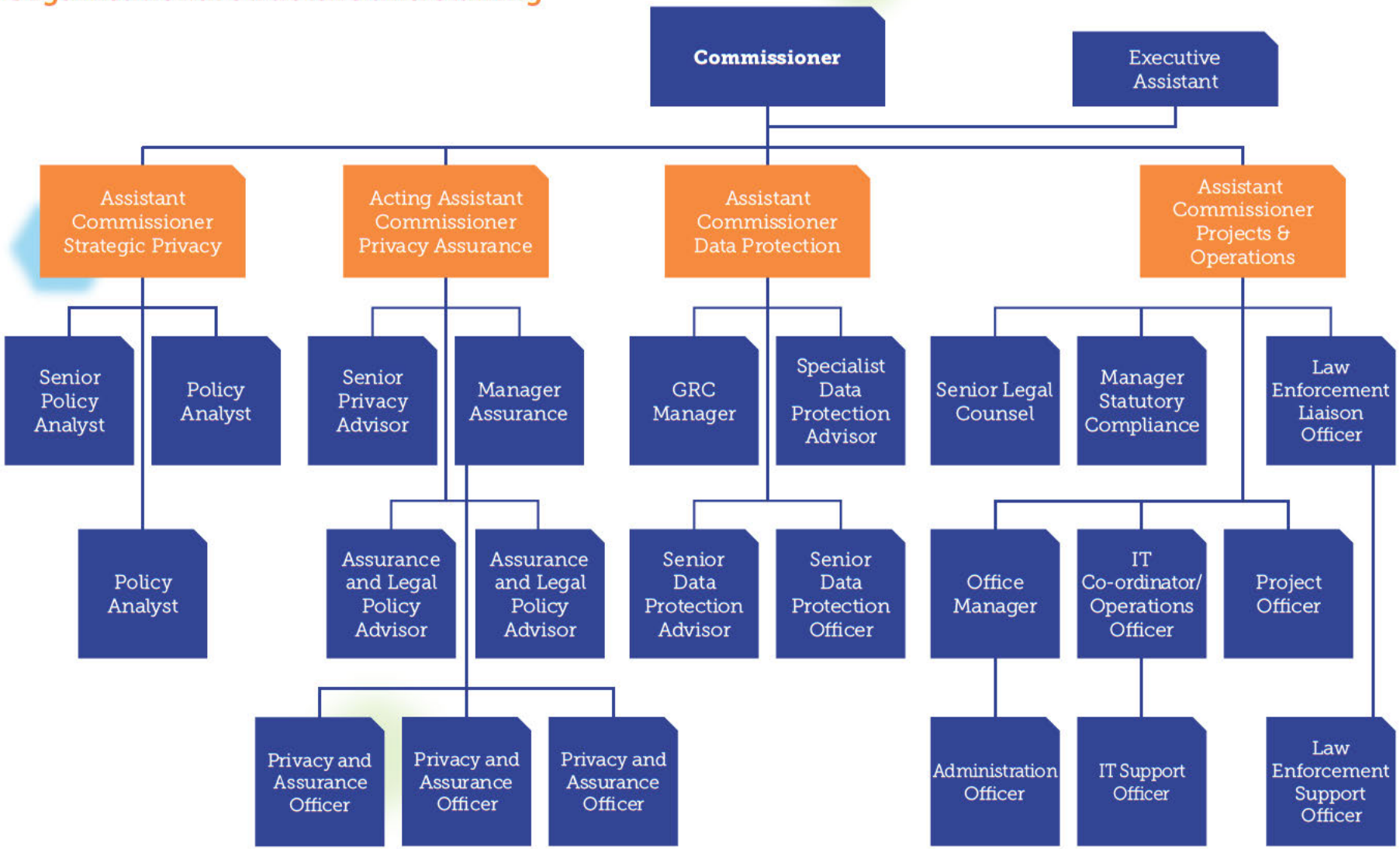
The Strategic Privacy team identified an opportunity to extend the online discussion of issues regarding information privacy through a Privacy Blog on the CPDP website. While CPDP regularly publishes formal guidance documents, the Privacy Blog acts as an alternative platform for less formal communication with stakeholders on new ideas and insights into topical areas related to information privacy. Blog content is sourced both internally from CPDP staff members, as well as externally through liaison with local universities and CPDP's Youth Advisory Group to seek input from students, academics and young people with an interest in information privacy.

Slack

In 2016 CPDP's Youth Advisory Group (YAG) was re-invigorated with new members and new objectives. The YAG identified a need to change the method of communication between members and CPDP staff running the group. Rather than using standard email, it was determined that an interactive platform for communication and project management would be more effective for this particular stakeholder group. The YAG now uses Slack, an online forum-style platform designed for group coordination and team work. As the group only meets face-to-face intermittently, maintaining online communication through Slack has increased the overall productivity and experience of the group.

About the Office of the Commissioner for Privacy and Data Protection

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 23 at 30 June 2017, comprised of 20.9 FTE, of which 1FTE was on secondment to the Department of Justice and Regulation, 3.9FTE on fixed term contracts and 16 FTE on-going members of the Victorian Public Service.

Gender	On-going	Fixed term	Secondment
Female	8.4	1	1
Male	8.4	1.9	1

Age	On-going	Fixed term	Secondment
Under 25		0.5	0
25 – 34	7	1	1
35 – 44	3.4	1	0
45 – 54	4	0	0
55 – 64	1.8	0.4	1
Over 64	1.6	0	0

Classification	On-going	Fixed term	Secondment
VPS2	0	1	0
VPS3	3	0.5	1
VPS4	1.4	1	0
VPS5	5	0.4	0
VPS6	5.6	0	1
STS	.8	0	0
Statutory Office Holder		1	

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. In 2016-17 the register was updated to incorporate the requirements of the revised 2016 Standing Directions.

Regular reporting tracks the status of CPDP projects, operations, compliance obligations and key stakeholder events. Reports are provided to the Audit and Finance Committee (A&FC).

CPDP reports on three measures in DPC's Public Sector Integrity output in Budget Paper Number 3. CPDP met or exceeded all of its 2016-17 targets (see Appendix C).

The Audit and Finance Committee met four times in 2016-17. 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 direction 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 (see the Stakeholder Engagement section of this report).

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 2016-17 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 2016-17.

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 one Freedom of Information request in 2016-17.

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)

Total expenditure on consultancies incurred during 2016-17 was $261,919 (excluding GST). Details of individual consultancies valued above $10,000 are outlined below.

Name of Consultancy Firm	Brief description of project	Type of consultancy based on standard criteria	Approved project fees (excl. GST)	Date of Contract
Lucinda Nolan	Review of DHHS out of home care	Review	$22,727	1/9/2016
Price Waterhouse-Coopers	Review of DHHS information governance	Review	$102,000	1/9/2016
University of Melbourne	De-identification project	Report	$35,000	1/12/2016
Lucinda Nolan	Review of DHHS information security practices	Review	$28,000	25/11/2016
Senate SHJ	Training Needs Analysis	Report	$22,000	1/5/2017
Sandra Beanham & Associates	VICPOL Survey Security Culture – Holdings Wave 3 report	Survey	$24,691	27/6/17
Sandra Beanham & Associates	VPDSF VPS Survey Plan June 2017	Survey	$20,501	27/6/17

Details of consultancies under $10,000

In 2015-16, there were 3 consultancies engaged during the year where the total fees payable to the individual consultancies was less than $10,000. The total expenditure incurred during 2016-17 in relation to these consultancies was $13,600 (excluding GST).

Information and communication technology expenditure

For the 2016-17 reporting period, CPDP had a total ICT expenditure of $165,379 with details shown below.

Business As Usual (BAU) ICT expenditure	Non-Business As Usual (non-BAU) ICT expenditure	Operational expenditure	Capital expenditure
103,676	61,703	33,959	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 attended the Privacy workshop and conference in New York in July 2016 and the International Conference of Data Protection and Privacy Commissioners in Morocco in October 2016.

The Assistant Commissioner Strategic Privacy also attended meetings of the Australasia Pacific Privacy Association in Singapore and Mexico.

Major contracts

The Commissioner did not enter into any contracts valued at more than $10 million in 2016-17.

Protected disclosures

The Commissioner received no disclosures made under the *Protected Disclosures Act 2012* during 2016-17.

Gifts, benefits and hospitality

The Commissioner maintains a register of gifts, benefits and hospitality. No declarable items were registered in 2016-17.

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 2016-17

Office of the Commissioner for Privacy and Data Protection

For the year ended 30 June 2017

Annual Financial Statements 2016-17

Contents ..... **Page**

Comprehensive operating statement
For the financial year ended 30 June 2017

Continuing operations	Notes	2017 $	2016 $
Income from transactions			
Grants	2.1	4,083,711	3,865,768
Total income from transactions		**4,083,711**	**3,865,768**
Expenses from transactions			
Employee benefits expenses	3.1	2,681,532	2,844,821
Depreciation	4.2	64,225	75,613
Other operating expenses	3.3	1,253,101	1,637,028
Total expenses from transactions		**3,998,857**	**4,557,462**
Net result from transactions (net operating balance)		**84,853**	**(691,694)**
Other economic flows included in net result			
Net gain/(loss) from the revaluation of leave liabilities		10,806	(19,233)
Total other economic flows included in net result		**10,806**	**(19,233)**
Net result		**95,660**	**(710,927)**
Comprehensive result		**95,660**	**(710,927)**

The accompanying notes form part of these financial statements.

Balance sheet
As at 30 June

	Notes	2017 $	2016 $
Assets			
Financial assets			
Receivables	5.1	672,521	1,098,644
Total financial assets		**672,521**	**1,098,644**
Non-financial assets			
Property, plant and equipment	4.1	162,854	212,078
Intangible assets	4.4	7,500	22,500
Prepayments	5.3	92,510	29,234
Total non-financial assets		**262,864**	**263,812**
Total assets		**935,385**	**1,362,456**
Liabilities			
Payables	5.2	133,703	583,150
Employee related provisions	3.2	721,410	794,693
Total liabilities		**855,113**	**1,377,843**
Net assets/(liabilities)		**80,272**	**(15,387)**
Equity			
Accumulated surplus/(deficit)		7,302	(88,358)
Contributed capital		72,971	72,971
Net worth		**80,272**	**(15,387)**

The accompanying notes form part of these financial statements.

Cash flow statement
For the financial year ended 30 June 2017

	Note	2017 $	2016 $
Cash flows from operating activities			
Receipts			
Receipts from government		4,509,833	4,582,875
Goods and services tax recovered from the ATO *		92,377	95,744
Total receipts		**4,602,210**	**4,678,619**
Payments			
Payments to suppliers and employees		(4,602,210)	(4,678,619)
Total payments		**4,602,210)**	**(4,678,619)**
Net cash flows from/(used in) operating activities	6.1	**-**	-
Net increase/(decrease) in cash and cash equivalents		**-**	-
Cash and cash equivalents at the end of the year		**-**	**-**

The accompanying notes form part of these financial statements.

Notes:

* GST recovered from the Australian Taxation Office is presented on a net basis.

Statement of changes in Equity
For the financial year ended 30 June 2017

	Contributed capital $	Accumulated surplus/(deficit) $	Total $
Balance at July 1 2015	72,971	622,569	**695,540**
Net result for the year		(710,927)	**(710,927)**
Balance at 30 June 2016	**72,971**	**(88,358)**	**(15,387)**
Net result for the year		95,660	**95,660**
Balance at 30 June 2017	**72,971**	**7,302**	**80,272**

The accompanying notes form part of these financial statements.

1. About this report

The Office of the Commissioner for Privacy and Data Protection (the 'Office') is an entity established under Part 6(1)(f) of the *Public Administration Act 2004* and this report is prepared in accordance with the *Privacy and Data Protection Act 2014* (the Act) under Division 3, Section 116. The Office operates under the auspices of the Department of Premier and Cabinet and reports to Parliament through the Special Minister of State. The Office's purpose, functions, powers and duties are set out in Part 1 and Part 3 of the Act.

Its principal address is:

The Office of the Commissioner for Privacy and Data Protection
Level 6
121 Exhibition Street
Melbourne VIC 3000

A description of the nature of its operations and its principal activities is included in the **"Report of operations"** which does not form part of these financial statements.

Basis of preparation

These financial statements are in Australian dollars and the historical cost convention is used unless a different measurement basis is specifically disclosed in the note associated with the item measured on a different basis. 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.

Consistent with the requirements of AASB 1004 *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.

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 applying Australian Accounting Standards (AASs) that have significant effects on the financial statements and estimates are disclosed in the notes under the heading: 'Significant judgement or estimates'. These financial statements cover the Office of the Commissioner for Privacy and Data Protection as an individual reporting entity.

Compliance information

These general purpose financial statements have been prepared in accordance with the *Financial Management Act 1994* and applicable Australian Accounting Standards (AASs) including 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 AASs paragraphs applicable to not-for-profit entities have been applied. Accounting policies selected and applied in these financial statements ensure that the resulting financial information satisfies the concepts of relevance and reliability, thereby ensuring that the substance of the underlying transactions or other events are reported.

2. Funding delivery of our services

INTRODUCTION

The Office has a number of legislated functions being principally:

- to promote an understanding and acceptance of the Information Privacy Principles (IPPs) and their objectives and 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 and 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; and
- to carry out information privacy related research.

STRUCTURE

2.1 Grants

2.1 Grants

	2017 $	2016 $
Grants from Department of Premier and Cabinet	4,083,711	3,865,768
Total income	**4,083,711**	**3,865,768**

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

Income from grants is recognised when the Office obtains control over the grant.

3. The cost of delivering our services

INTRODUCTION

This section provides an account of the expenses incurred by the Office in delivering services and outputs.

STRUCTURE

3.1 Employee benefits expense

	2017 $	2016 $
Salaries and wages, annual leave and long service leave	2,465,471	2,638,523
Defined contribution superannuation expense	200,904	188,531
Defined benefit superannuation expense	15,157	17,766
Total employee benefits	**2,681,532**	**2,844,821**

Employee benefits comprise 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 in relation to superannuation is employer contributions for members of both defined benefit and defined contribution superannuation plans that are paid or payable during the reporting period. The Office does not recognise any defined benefit liabilities because it has no legal or constructive obligation to pay future benefits relating to its employees. Instead, the Department of Treasury and Finance discloses in its annual financial statements the net defined benefit cost related to the members of these plans as an administered liability (on behalf of the State of Victoria as the sponsoring employer).

Provisions

Provision is made for benefits accruing to employees in respect of wages and salaries, annual leave and long service leave (LSL) for services rendered to the reporting date and recorded as an expense during the period the services are delivered.

3.2 Employee benefits in the balance sheet

	2017 $	2016 $
Current provisions:		
Annual leave		
Unconditional and expected to settle within 12 months	173,468	184,378
Unconditional and expected to settle after 12 months	53,225	27,869
Long service leave		
Unconditional and expected to settle within 12 months	64,899	84,934
Unconditional and expected to settle after 12 months	318,141	407,453
Provisions for on-costs		
Unconditional and expected to settle within 12 months	34,055	20,785
Unconditional and expected to settle after 12 months	42,804	42,603
Total current provisions	**686,593**	**768,022**
Non current provisions		
Employee benefits - long service leave	31,409	24,061
Employee benefits - long service leave-on costs	3,408	2,610
Total non-current provisions	**34,817**	**26,671**
Total provisions	**721,410**	**794,693**

Wages and salaries, annual leave and sick leave

Liabilities for wages and salaries (including non-monetary benefits, annual leave and on-costs) are recognised as part of the employee benefit provision as current liabilities, because the Office does not have an unconditional right to defer settlements of these liabilities.

The liability for salaries and wages are recognised in the balance sheet at remuneration rates which are current at the reporting date. As the Office expects the liabilities to be wholly settled within 12 months of reporting date, they are measured at undiscounted amounts.

The annual leave liability is classified as a current liability and measured at the undiscounted amount expected to be paid, as the 'office' does not have an unconditional right to defer settlement of the liability for at least twelve months after the end of the reporting period.

No provision has been made for sick leave as all sick leave is non-vesting and it is not considered probable that the average sick leave taken in the future will be greater than the benefits accrued in the future. As sick leave is non-vesting, an expense is recognised in the Statement of Comprehensive Income as it is taken.

Unconditional LSL is disclosed 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; or
- 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 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' in the net result.

3.3 Other operating expenses

	2017 $	2016 $
Purchase of services	477,284	628,844
Information technology expenses	130,629	301,175
Operating lease payments [(i)]	301,742	230,463
Other occupancy costs [(ii)]	94,064	143,124
Other supplies and services	249,382	333,423
Total other operating expenses	**1,253,101**	**1,637,028**

Notes:

(i) Operating lease payments are recognised 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, in the Office's case they relate directly to the Exhibition Street premises.

(ii) Other occupancy costs represent the remainder of the expenses relating to the Exhibition Street premises that are not included as part of the operating lease payments.

Purchases of services generally represent the day-to-day running costs incurred in normal operations of the Office. Supplies and services are recognised as an expense in the reporting period in which they are incurred.

The Department of Premier and Cabinet has been centrally funding the services provided to the Office for nominal consideration. The services that are utilised include the use of the financial systems, payroll systems, accounts payable and asset register.

4. Key assets available to support output delivery

INTRODUCTION

The Office controls property, plant and equipment that are utilised in fulfilling its objectives and conducting its activities. They represent the key resources that have been entrusted to the Office to be utilised for delivery of those outputs.

STRUCTURE

4.1 Property, plant and equipment

	Gross carrying amount		Accumulated depreciation		Net carrying amount	
	2017 $	2016 $	2017 $	2016 $	2017 $	2016 $
Leasehold improvements	226,071	226,071	(97,446)	(72,108)	128,626	153,964
Office and computer equipment	93,945	93,945	(59,716)	(35,830)	34,229	58,115
Net carrying amount	**320,017**	**320,017**	**(157,162)**	**(107,937)**	**162,854**	**212,078**

Initial recognition

Items of property, plant and equipment 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.

Leasehold improvements

The cost of leasehold improvements is capitalised and depreciated over the shorter of the remaining term of the lease or their estimated useful lives.

The initial cost for non-financial physical assets under a finance lease is measured at amounts equal to the fair value of the leased asset or, if lower, the present value of the minimum lease payments, each determined at the inception of the lease.

Office and computer equipment

Office and computer equipment is valued using the historical cost method. Historical cost is used due to the short useful life of office and computer equipment.

4.2 Depreciation

	2017 $	2016 $
Leasehold improvements	25,338	36,727
Office and computer equipment	23,886	23,887
Intangible assets	15,000	15,000
Total depreciation	**64,225**	**75,613**

All property, plant and equipment with finite useful lives, are depreciated. Depreciation is calculated on a straight line basis, at rates that allocate the asset's value, less any estimated residual value, over its expected useful life. Depreciation begins when the asset is available for use, that is, when it is in the location and condition necessary for it to be capable of operating in the manner intended by management.

Typical estimated useful lives for the Office's different asset classes for current and prior years are included in the table below.

Asset class	Estimated useful life
Leasehold improvements	5-8 years
Office and computer equipment	3-5 years
Intangible assets	3-4 years

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

Property, plant and equipment, are tested for impairment whenever there is an indication that the asset may be impaired. 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 it can be debited to an asset revaluation surplus amount applicable to that class of asset.

4.3 Reconciliation of the carrying amounts of assets by class

	Leasehold improvements $	Office and computer equipment $	Total $
2017			
Carrying amount at the start of the year	153,964	58,115	212,079
Depreciation expenses	(25,338)	(23,886)	(49,225)
Carrying amount at the end of the year	128,626	34,229	162,855
2016			
Carrying amount at the start of the year	190,691	82,002	272,693
Depreciation expenses	(36,727)	(23,887)	(60,613)
Carrying amount at end of year	153,964	58,115	212,079

The Office of the Commissioner for Privacy and Data Protection incurred no disposals, additions or transfers of assets between classes during the reporting period.

4.4 Intangible assets

	Computer software	
	2017 $	2016 $
Gross carrying amount	45,000	45,000
Accumulated depreciation	(37,500)	(22,500)
Net book value at the end of financial year	7,500	22,500

Initial recognition-intangible assets

Purchased intangible assets are initially recognised at cost. When the recognition criterion in AASB 138 *Intangible Assets* is met, intangible assets with finite useful lives are carried at cost less accumulated depreciation.

Subsequent measurement

Intangible assets with finite useful lives are depreciated as an expense from transactions on a straight line basis over the asset's useful life. Depreciation begins when the asset is available for use, that is, when it is in the location and condition necessary for it to be capable of operating in the manner intended by management.

5. Other assets and liabilities

INTRODUCTION

This section sets out those assets and liabilities that arose from the Office in delivering services and outputs.

STRUCTURE

5.1 Receivables

	2017 $	2016 $
Contractual		
Debtors	33,987	-
Statutory		
Amounts owing from Victorian government	635,973	1,049,401
GST recoverable	2,560	49,242
Total receivables	**672,521**	**1,098,643**
Represented by:		
Current receivables	637,704	1,071,972
Non-Current receivables	**34,817**	**26,671**

Contractual receivables are classified as financial instruments and categorised as receivables. They are initially recognised at fair value plus any directly attributable transaction costs. Subsequent to initial measurement they are measured at amortised cost using the effective interest method, less any impairment.

There are no financial assets that have had their terms renegotiated so as to prevent them from being past due or impaired, and they are stated at the carrying amounts as indicated.

Statutory receivables do not arise from contracts and are initially recognised at fair value plus any directly attributable transaction costs. Subsequent to initial measurement they are measured at amortised cost using the effective interest method, less any impairment and are not classified as financial instruments.

5.2 Payables

	2017 $	2016 $
Contractual		
Creditors and accruals	118,558	574,793
Statutory		
Amounts payable to other government agencies	15,145	8,357
Total payables	**133,703**	**583,150**
Represented by:		
Current	133,703	583,150
Non-Current	-	-

Contractual payables are classified as financial instruments and measured at amortised cost. Accounts payable represent liabilities for goods and services provided to the Office prior to the end of the financial year that are unpaid.

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 contracts.

5.3 Prepayments

	2017 $	2016 $
Prepayments	92,510	29,234
Total prepayments	**92,510**	**29,234**

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. Prepayments at the end of the financial year relate to office occupancy, WorkCover insurance, supplies and services.

6. Financing our operations

INTRODUCTION

This section provides information on the sources of finance utilised during the Office's operations.

STRUCTURE

6.1 Reconciliation of the net result for the period to cash flow from operating activities

6.2 Commitments for expenditure

6.1 Reconciliation of the net result for the period to cash flow from operating activities

	2017 $	2016 $
Net result for the period	**95,660**	**(710,927)**
Non-cash movements		
Depreciation and amortisation of non-current assets	64,225	75,613
Movements in assets and liabilities		
(Increase)/decrease in receivables	426,123	621,566
(Increase)/decrease in other non-financial assets	(63,277)	50,766
(Decrease)/Increase in payables	(449,449)	(22,255)
(Decrease)/Increase in provisions	(73,283)	(14,763)
Net cash flows from (used in) operating activities	**-**	**-**

6.2 Commitments for expenditure

Nominal amounts	Less than one year $	1-5 years $	Greater than 5 years $	Total $
2017				
Operating and lease commitments payable*				
Total commitments (inclusive of GST)	**458,782**	**2,020,982**	**-**	**2,479,764**
Less GST recoverable	(41,707)	(183,726)	-	(225,433)
Total commitments (exclusive of GST)	**417,075**	**1,837,256**	**-**	**2,254,331**
2016				
Operating and lease commitments payable*				
Total commitments (inclusive of GST)	**401,788**	**1,773,388**	**488,278**	**2,663,454**
Less GST recoverable	(36,526)	(161,217)	(44,389)	(242,132)
Total commitments (exclusive of GST)	**365,262**	**1,612,171**	**443,889**	**2,421,322**

Notes:

* Operating and lease commitments payable include 'operating lease payments' and certain 'other occupancy costs' that arise due to a contractual requirement as part of the Exhibition Street office facilities lease.

Commitments for future expenditure include operating and capital commitments arising from contracts. These commitments are recorded below at their nominal value and inclusive of GST. Where it is considered appropriate and provides additional 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.

7. Risks, contingencies and valuation judgements

INTRODUCTION

The Office is exposed to risk from its activities and outside factors. In addition, it is often necessary to make judgements and estimates associated with recognition and measurement of items in the financial statements. This section sets out financial instrument specific information, as well as those items that are contingent in nature or require a higher level of judgement to be applied.

STRUCTURE

7.1 Financial instruments specific disclosures

Introduction

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 (for example taxes, fines and penalties). Such assets and liabilities do not meet the definition of financial instruments in AASB 132 *Financial Instruments: Presentation*

Categories of financial instruments

Receivables

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, receivables are measured at amortised cost using the effective interest method, less any impairment.

Financial liabilities at amortised cost

Financial instrument liabilities are 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 using the effective interest rate method.

Offsetting financial instruments

Financial instrument assets and liabilities are offset and the net amount presented in the balance sheet when, and only when, there is a legal right to offset the amounts and an intention either to settle on a net basis or to realise the asset and settle the liability simultaneously.

7.2 Categorisation of financial instruments

			2017 $	2016 $
Financial assets	**Note**	**Category**		
Receivables *	5.1	Receivables	33,987	-
			33,987	**-**
Financial liabilities				
Payables	5.2	Financial liabilities at amortised cost	118,558	574,793
			118,558	**574,793**

Note:

* Receivables disclosed exclude statutory receivables (i.e. amounts receivable from government departments and GST recoverable)

7.3 Financial risk management objectives and policies

As a whole, the Office's financial risk management program seeks to manage the risks arising from volatility in financial instruments.

The Office's main financial risks include credit risk, liquidity risk and market risk. The Office manages these financial risks in accordance with its financial risk management policy.

Credit risk

Credit risk associated with the Office's financial assets is minimal because the main debtor is other departments within the Victorian Government.

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.

Market risk

The Office's exposure to market risk is deemed insignificant based on prior periods' data and a current assessment of risk.

7.4 Contingent assets and contingent liabilities

Contingent assets and contingent liabilities are not recognised in the balance sheet but are disclosed and, if quantifiable, are measured at nominal value.

Contingent assets and liabilities are presented inclusive of GST receivable or payable respectively.

Contingent assets

Contingent assets are possible assets that arise from past events, whose existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the control of the entity.

These are classified as either quantifiable, where the potential economic benefit is known, or non-quantifiable.

There were no contingent assets based on the above definitions relating to Office of the Commissioner for Privacy and Data Protection as at 30 June 2017.

Contingent liabilities

Contingent liabilities are:

- possible obligations that arise from past events, whose existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the control of the entity; or
- present obligations that arise from past events but are not recognised because:
- it is not probable that an outflow of resources embodying economic benefits will be required to settle the obligations; or
- the amount of the obligations cannot be measured with sufficient reliability.

Contingent liabilities are also classified as either quantifiable or non-quantifiable.

There were no contingent liabilities based on the above definitions relating to Office of the Commissioner for Privacy and Data Protection as at 30 June 2017.

8. Other disclosures

INTRODUCTION

This section includes additional material disclosures required by accounting standards or otherwise, for the understanding of this financial report.

STRUCTURE

8.1 Subsequent events

Restructuring of administrative arrangements

The Freedom of Information Commission and the Office of the Commissioner for Privacy and Data Protection (CPDP), which are both portfolio entities of the Department of Premier and Cabinet are combined to form the Office of the Victorian Information Commissioner from 1 September 2017. All assets and liabilities of CPDP were transferred to the Victorian Information Commissioner and the new entity has taken over the services previously provided by CPDP.

8.2 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 for Office of the Commissioner for Privacy and Data Protection are as follows

Position	Names	Term
Special Minister of State	The Hon. Gavin Jennings MP	1 July 2016 to 30 June 2017
Commissioner	David Watts	1 July 2016 to 30 June 2017

The persons who acted in the position of Responsible Minister during 1 July 2016 to 30 June 2017 were:

- The Hon Daniel Andrews MP and The Hon James Merlino MP, who acted in the office of the Special Minister of State in the absence of The Hon Gavin Jennings MLC

Remuneration received or receivable by the Accountable Officer in connection with the management of the Office during the reporting period was in the range of $300,000-$309,999 ($300,000-$309,999 in 2015-16).

8.3 Remuneration of Executives

Other than the Responsible Ministers and Accountable Officer there were no other executive officers during the reporting period.

8.4 Related Parties

The Office of the Commissioner for Privacy and Data Protection is a wholly owned and controlled entity of the State of Victoria.

Related Parties of the Office include:

- all key management personnel and their close family members and personal business interests (controlled entities, joint ventures and entities they have significant influence over);
- all cabinet ministers and their close family members; and
- all departments and public sector entities that are controlled and consolidated into the whole of state consolidated financial statements.

Significant transactions with government-related entities

The Office of the Commissioner for Privacy and Data Protection received grants from the Department of Premier and Cabinet totaling $4.1 million (2016 was $3.9 million).

The Key Management Personnel (KMP) of the Office of the Commissioner for Privacy and Data Protection included the Special Minister of State, The Hon Gavin Jennings MP and officers listed below:

Key management personnel	Role
David Watts	Commissioner
Gary Sauvarin	Assistant Commissioner Projects and Operations

The compensation detailed below excludes the salaries and benefits the Portfolio Minister receives. The Minister's remuneration and allowances is set by the *Parliamentary Salaries and Superannuation Act 1968* and is reported within the Department of Parliamentary Services' Financial Report.

Key management personnel - remuneration

	2017 $
Short-term employee benefits	450,710
Post-employment benefits	39,256
Other long-term benefits	8,574
Total	**498,540**

Remuneration comprises employee benefits in all forms of consideration paid, payable or provided by the entity, or on behalf of the entity, in exchange for services rendered, and is disclosed in the following categories.

Short-term employee benefits include amounts such as wages, salaries, annual leave or sick leave that are usually paid or payable on a regular basis, as well as non-monetary benefits such as allowances and free or subsidised goods or services.

Post-employment benefits include pensions and other retirement benefits paid or payable on a discrete basis when employment has ceased.

Other long-term benefits include long service leave, other long-service benefit or deferred compensation.

Transactions with key management personnel and other related parties

Given the breadth and depth of state government activities, related parties transact with the Victorian public sector in a manner consistent with other members of the public. Further employment of processes within the Victorian public sector occur on terms and conditions consistent with the *Public Administration Act 2004*, codes of conduct, and standards issued by the Victorian Public Sector Commission. Procurement processes occur on terms and conditions consistent with the Victorian Government Procurement Board requirements.

Outside of normal citizen-type transactions, there were no related party transactions that involved key management personnel and their close family members. No provision has been required, nor any expense recognised, for impairment of receivables from related parties.

8.5 Remuneration of auditors

	2017 $	2016 $
Audit fees paid or payable to the Victorian Auditor-General's Office		
Audit of the Victorian Privacy Commissioner	-	1,500
Audit of the Annual Financial Statements	15,900	15,500
Total	**15,900**	**17,000**

8.6 Accounting standards that are not yet effective

These AASs have been published, but are not mandatory for the 2016-17 reporting period. The Department of Treasury and Finance has assessed the impact of all these new standards and advised the Inspectorate of their applicability and early adoption where applicable. The table below details the AASs issued but not yet effective for the 2016-17 reporting period.

Standard/ Interpretation	Summary	Applicable for annual reporting periods beginning on	Impact on public sector entity financial statements
AASB 2010-7 *Amendments to Australian Accounting Standards arising from AASB 9* (December 2010)	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 (OCI); and Other fair value changes are presented in profit and 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.	1 Jan 2018	The assessment has identified that the financial impact of available for sale (AFS) assets will now be reported through other comprehensive income (OCI) and no longer recycled to the profit and loss. Changes in own credit risk in respect of liabilities designated at fair value through profit and loss will now be presented within other comprehensive income (OCI). Hedge accounting will be more closely aligned with common risk management practices making it easier to have an effective hedge. For entities with significant lending activities, an overhaul of related systems and processes may be needed.
AASB 15 *Revenue from Contracts with Customers*	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.	1 Jan 2018	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.

Standard/ Interpretation	Summary	Applicable for annual reporting periods beginning on	Impact on public sector entity financial statements
AASB 2015-8 *Amendments to Australian Accounting Standards – Effective Date of AASB 15*	This Standard defers the mandatory effective date of AASB 15 from 1 January 2017 to 1 January 2018.	1 Jan 2018	This amending standard will defer the application period of AASB 15 for for-profit entities to the 2018-19 reporting period in accordance with the transition requirements.
AASB 2016-7 *Amendments to Australian Accounting Standards – Deferral of AASB 15 for Not-for-Profit Entities*	This Standard defers the mandatory effective date of AASB 15 for not-for-profit entities from 1 January 2018 to 1 January 2019.	1 Jan 2019	This amending standard will defer the application period of AASB 15 for not-for-profit entities to the 2019-20 reporting period.
AASB 16 *Leases*	The key changes introduced by AASB 16 include the recognition of most operating leases (which are current not recognised) on balance sheet.	1 Jan 2019	The assessment has indicated that as most operating leases will come on balance sheet, recognition of the right-of-use assets and lease liabilities will cause net debt to increase. Rather than expensing the lease payments, depreciation of right-of-use assets and interest on lease liabilities will be recognised in the income statement with marginal impact on the operating surplus. There will be no change for lessors.
AASB 2016-4 *Amendments to Australian Accounting Standards – Recoverable Amount of Non-Cash-Generating Specialised Assets of Not-for-Profit Entities*	The standard amends AASB 136 *Impairment of Assets* to remove references to using depreciated replacement cost (DRC) as a measure of value in use for not-for-profit entities.	1 Jan 2017	The assessment has indicated that there is minimal impact. Given the specialised nature and restrictions of public sector assets, the existing use is presumed to be the highest and best use (HBU), hence current replacement cost under AASB 13 *Fair Value Measurement* is the same as the depreciated replacement cost concept under AASB 136.
AASB 1058 *Income of Not-for-Profit Entities*	This standard replaces AASB 1004 *Contributions* and establishes revenue recognition principles for transactions where the consideration to acquire an asset is significantly less than fair value to enable to not-for-profit entity to further its objectives.	1 Jan 2019	The assessment has indicated that revenue from capital grants that are provided under an enforceable agreement that have sufficiently specific obligations, will now be deferred and recognised as performance obligations are satisfied. As a result, the timing recognition of revenue will change.

Accountable Officer's and Chief Financial Officer's declaration

Office of the Commissioner for Privacy and Data Protection

Accountable Officer's and Chief Financial 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 5.2 of the Standing Directions of the Minister for Finance under the 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, cash flow statement, statement of changes in equity and notes to the financial statements, presents fairly the financial transactions during the year ended 30 June 2017 and financial position of the Office as at 30 June 2017. At the time of signing, we are not aware of any circumstance, which would render any particulars included in the financial statements to be misleading or inaccurate.

We authorise the attached financial statements for issue on 26 September 2017.

Joseph Yeung
Chief Financial Officer

Melbourne
26 September 2017

Sven Bluemmel
Information Commissioner

Melbourne
26 September 2017

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 & Financial Reporting Directions		
Report of Operations		
Charter and purpose		
FRD 22H	Manner of establishment and the relevant Ministers	Page 8
FRD 22H	Objectives, functions, powers and duties	Page 8 – 9
FRD 22H	Nature and range of services provided	Page 10 – 31
Management and structure		
FRD 22H	Organisational structure	Page 33
Financial and other information		
FRD 8D	Performance against output performance measures	Page 43
FRD 10A	Disclosure index	Page 40 – 41
FRD 12B	Disclosure of major contracts	Page 37
FRD 15D	Executive officer disclosures	Page 37
FRD 22H	Employment and conduct principles	Page 34
FRD 22H	Occupational health and safety policy	Page 34
FRD 22H	Summary of the financial results for the year	Page 38 – 61
FRD 22H	Application and operation of Freedom of Information Act 1982	Page 35
FRD 22H	Application and operation of the Protected Disclosures Act 2012	Page 37
FRD 22H	Details of consultancies over $10 000	Page 36
FRD 22H	Details of consultancies under $10 000	Page 36
FRD 22H	Statement of availability of other information	Page 37
FRD 24C	Reporting of officebased environmental impacts	Page 35
FRD 29B	Workforce Data disclosures	Page 34
FRD 22H	Disclosure of ICT expenditure	Page 36
SD 3.7.1	Attestation for compliance with Ministerial Standing Direction 3.7.1	Page 64

Legislation	Requirement	Page Reference
Financial Statements		
Declaration		
SD 5.2.2	Declaration in financial statements	Page 61
Other requirements under Standing Direction 5.2		
SD 5.2.1(a)	Compliance with Australian accounting standards and other authoritative pronouncements	Page 44
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 57
FRD103F	Non-Financial Physical Assets	Page 49
FRD110	Cash Flow Statements	Page 42

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

Appendix B — Attestation complying with Standing Direction 3.7.1

ATTESTATION COMPLYING WITH STANDING DIRECTION 3.7.1

I, Sven Bluemmel, certify that the Office of the Commissioner for Privacy and Data Protection has complied with the Ministerial Standing Direction 3.7.1 – Risk Management Framework and Processes during 2016/17. The Office of the Commissioner for Privacy and Data Protection Audit and Finance Committee has verified this.

SVEN BLUEMMEL
Information Commissioner

26 September 2017

Appendix C — Budget Paper 3

Budget Paper Number Three (BP3) Output Performance 2016-17

CPDP's performance measures are included in the Department of Premier and Cabinet's public sector integrity output.

Performance measures	Unit of measure	2016-17 actual	2016-17 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	✓
High levels of satisfaction by users of privacy training. Satisfaction levels are expected to move towards target following the introduction of data security training.					
Timeliness					
Responses within 15 days to written enquiries relating to the legislated responsibilities of the Commissioner of Privacy and Data Protection.	per cent	96.0	90.0	+6.0	✓
Systems to monitor and respond to enquiries are working effectively. Target is expected to be harder to achieve in the future due to the number and complexity of enquiries increasing as Victorian citizens and the VPS become aware of the provisions of the CPDP legislation.					

Note:

1. ✓ 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].

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

Commissioner
for Privacy and
Data Protection

VICTORIA
State
Government