information and privacy commission
new south wales

Revenue NSW

***Privacy and Personal Information Protection Act* – Compliance Report**

March 2020

Contents

Abbreviations

The following table lists the commonly used abbreviations within this report.

Acronym or abbreviation	Explanation
ARC	Audit and Risk Committee
DCS	Department of Customer Service
DFSI	Department of Finance, Services and Innovation
The Framework	DFSI Privacy Governance Framework
HRIP	*Health Records and Information Privacy Act 2002*
HPP	Health Privacy Principle
IPC	Information and Privacy Commission
IPP	Information Protection Principle
GIPA	*Government Information (Public Access) Act 2009*
RNSW	Revenue NSW
PMP	Privacy Management Plan
PPIP Act	*Privacy and Personal Information Protection Act 1998*
WDO	Work and Development Order

1 Purpose

Revenue NSW (RNSW) collects, uses and stores personal information in association with the administration of its functions in collecting revenues, administering grants and recovering debts on behalf of the people of NSW in accordance with the legislation it is responsible to administer.[1] RNSW is an office within the Department of Customer Service. For the purposes of the *Government Sector Employment Act 2013* (GSE Act), RNSW is not a separate agency or executive agency under the GSE Act.[2]

On 22 November 2018, RNSW voluntarily notified the Privacy Commissioner of an inadvertent disclosure of personal information arising from a report made to its Minister. At the time, RNSW informed the Privacy Commissioner of the actions it had taken to investigate and address the inadvertent disclosure. Subsequent to this advice, media reported on the inadvertent disclosure, which included personal information relevant to Mr Michael Daley, MP.[3]

As a consequence of the media reports, the Privacy Commissioner determined to make further inquiries of RNSW about its general information management governance in so far as it relates to the management of disclosure of personal information. Accordingly, this investigation by way of audit examined the processes, practices and governance in place for the management of, and compliance with, the information protection principles (IPPs) by RNSW in relation to the handling and management of personal information under the *Privacy and Personal Information Protection Act 1998* (PIPA Act) relevant to the disclosure of personal information.

Section 36 of the PPIP Act provides for the general functions of the Privacy Commissioner. In particular section 36(2) provides that the Privacy Commissioner's functions include promoting the adoption of, and monitoring compliance with, the information protection principles. Those functions include conducting such inquiries, and making such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate.

2 Scope of the Audit

The purpose of the investigation by way of an audit was to assess the practices, processes and governance arrangements of RNSW in fulfilling its responsibilities under Division 1 of Part 2 of the PPIP Act.

In accordance with section 39 of the PPIP Act, the Privacy Commissioner has determined the procedures to be followed in exercising her functions under the PPIP Act.

Following a preliminary assessment and informed by the voluntary notification by RNSW, and matters relevant to that notification, it was determined by the Privacy Commissioner that this necessitated consideration of whether RNSW had appropriate arrangements in place for the handling of personal information and the management of the disclosure of personal information under the PPIP Act.

Accordingly, the investigation was conducted by way of an audit of RNSW's:

- processes to manage the disclosure of personal information

[1] Legislation administered by Revenue NSW is available at https://www.revenue.nsw.gov.au/about/legislation-and-rulings/legislation

[2] Schedule 1 Government Sector Employment Act 2013

[3] https://www.smh.com.au/politics/nsw/labor-leader-s-staff-used-secret-hotline-to-blame-wife-for-speeding-20190207-p50wdj.html

- practices in place for the management of privacy breaches
- training and guidance for officers of RNSW relevant to privacy management.

This investigation was limited to the general information management governance of RNSW as it relates to the management of disclosure of personal information under the PPIP Act and did not consider all compliance requirements under the PPIP Act. Specifically, this report did not assess or consider individual complaints about the handling of personal information by RNSW or the specific inadvertent disclosure that informed the decision to undertake this investigation by way of audit.

Accordingly, while informed by the notification by RNSW of an inadvertent disclosure, the focus of this inquiry was on the ongoing practices of RNSW. This is because the Privacy Commissioner was satisfied that RNSW had taken reasonable steps to manage the inadvertent disclosure consistent with the voluntary reporting arrangements adopted in NSW.[4]

In undertaking this investigation, the Privacy Commissioner notes that complaints about the inadvertent disclosure were also the subject of consideration by other authorities, being the NSW Police and NSW Independent Commission against Corruption (ICAC).[5]

3 Executive summary

RNSW is the state's principal revenue management agency. It came into effect on 31 July 2017, following a name change from the Office of State Revenue and State Debt Recovery Office. RNSW is part of the Department of Customer Service.[6]

NSW Government agencies, like RNSW, collect personal and health information from citizens in order to deliver important services in health, education and other areas. For RNSW this means that it collects personal information of citizens associated with the administration of its revenue management function which includes:

- administering state taxation
- managing fines
- administering grants and subsidies
- recovering debt.[7]

As part of its functions as a state debt collector, it is also likely that the agency collects health information associated with its Work and Development Order (WDO) Program either directly, or indirectly, as part of its approval of WDO applications or as part of any compliance activity it may undertake associated with the program. The program enables citizens to complete unpaid work, education, treatment or counselling to resolve their fines. Eligibility for a WDO is for citizens who:

---

[4] No mandatory reporting data breach scheme operated in NSW at the time of the inadvertent disclosure. The Privacy Commissioner encourages voluntary reporting in NSW and has issued guidance to support agencies available at https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification

[5] https://www.parliament.nsw.gov.au/lcdocs/transcripts/2240/Transcript%20-%2012%20September%2019%20-%20UNCORRECTED%20-%20PC%206%20-%20Customer%20Service%20-%20Dominello.pdf

[6] About Us https://www.revenue.nsw.gov.au/about/who-we-are

[7] Revenue NSW Annual Report 2017-18 at https://www.revenue.nsw.gov.au/help-centre/resources-library/year_in_review.pdf

- have serious medical, mental health or addiction problems
- have a cognitive impairment or intellectual disability
- are homeless or are experiencing severe financial hardship
- may be disproportionately impacted by fines debt.[8]

Accordingly, it is likely that the scope of the information that RNSW collects about citizens in the exercise of its functions substantively includes personal information as provided for by the PPIP Act but is also likely to extend to include information that may be considered as personal health information under the *Health Records and Information Privacy Act 2002* (HRIP Act).

An agency's effective ability to provide these services therefore depends on the ability for citizens to trust that as the custodian of their personal, and at times sensitive information, government agencies will collect, disclose, manage and secure their information in a way that is respectful of their privacy.

This requires the promotion of trust, confidence and leadership in the way that personal information is managed by agencies. This is enabled by strong and effective privacy policy, practice and frameworks that demonstrate a commitment to privacy which promotes good privacy governance within agencies to create and embed a culture that respects privacy and treats personal information as a valuable asset.[9] This requires a culture which is respectful of privacy issues, values and protects personal information necessarily led from the top down.

This review observed that RNSW approaches its privacy culture by having in place governance structures to support reporting, address sensitive data, use of ongoing audit and monitoring processes and information management, governance arrangements in place for personal information management. This includes a mechanism for executive oversight and monitoring of compliance with those practices. Having these practices in place is an important step in achieving and building citizen trust and confidence in the personal information handling practices of RNSW. However, importantly they must be supplemented by continuous promotion by the senior leadership to ensure that the cultural objectives are embedded within the Agency.

4 Background

The Privacy Commissioner, in accordance with her function under section 36(2)(l) of the PPIP Act, initiated an investigation into the privacy matters related to the handling of personal information by RNSW. Informed by an inadvertent disclosure of personal information that was the subject of media reports, the inquiry was directed at the appropriateness of practices and governance in place for the management of personal information.

Sound governance arrangements and robust policies and practices in conjunction with training and guidance are integral to a robust privacy compliance environment. In this context, the Privacy Commissioner identified potential risks in the processes and practices for the management of personal information.

This investigation concerns RNSW as the agency responsible for collecting, using, disclosing and securing personal information under the PPIP Act.

---

[8] Revenue NSW Annual Report 2017 -18 at https://www.revenue.nsw.gov.au/help-centre/resources-library/year_in_review.pdf

[9] OAIC Privacy Code for Government Agencies, May 2017 at https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code/

In June 2019, the Privacy Commissioner informed RNSW she was to conduct an investigation by way of an audit.

At the time that this investigation commenced RNSW was within the Department of Finance, Services and Innovation (DFSI) cluster. It is noted that consequent upon Machinery of Government Changes which took effect on and from 1 July 2019, DFSI ceased to exist as a standalone department and its functions were absorbed into the newly formed Department of Customer Service (DCS). Accordingly, from 1 July 2019, RNSW was within the DCS cluster. Within RNSW privacy management is supported by the Privacy Unit of DCS (formerly DFSI).[10]

The investigation was conducted in accordance with section 39 of the PPIP Act, which provides that the Privacy Commissioner may determine the procedures to be followed in exercising her functions under the PIPP Act. The Privacy Commissioner determined that an audit approach would be appropriate.

The information privacy principles (IPPs) are at Appendix A.

This report outlines the findings and proposed recommendations as a result of the audit.

5 Conduct of the audit and provision of compliance report

In conducting the investigation by way of audit, representatives of the IPC met with representatives of RNSW, and assessed RNSW's policies and practices for management of the IPPs under the PPIP Act. RNSW also made available to the IPC a suite of its policies relevant to the management of personal information under the PPIP Act.

A draft report was provided to RNSW for comment. RNSW responded on 8 January 2020. That response has been considered and taken into account in the finalisation of this report. I welcome RNSW's response to the recommendations made in this report and its commitment to advancing positive privacy practices across the organisation.

In finalising this report I acknowledge the advice from RNSW in respect of recommendations 13 and 18 which may now be impacted by the *Fines Amendment Act 2019* which was assented to on 21 November 2019. I note that as at the finalisation of this report those amendments had yet not come into force. Accordingly, I note that the recommendations made in 13 and 18 may necessarily require amendment to reflect the particular notification requirements provided by the amendments to the *Fines Amendment Act 2019* which sets out its own notification requirements.

This final report addresses where relevant, the issues raised in the response from RNSW and outlines the audit observations and associated recommendations.

6 Acknowledgments

The Privacy Commissioner and the Information and Privacy Commission (IPC) acknowledge the co-operation and assistance afforded by RNSW and its representatives during the course of this audit.

10. Effective 1 July 2019, following Machinery of Government Changes, DFSI ceased to exist as a separate agency and replaced by the new Department of Customer Service. See https://www.legislation.nsw.gov.au/regulations/2019-159.pdf

7 Methodology

7.1 Audit sample

The audit involved:

- a sample assessment of RNSW's privacy management practices for some aspects of the IPPs under the PPIP Act
- a review of publicly available information about RNSW
- IPC attendance at the offices of RNSW
- access to RNSW's systems, policies, procedures and relevant representatives.

During the course of this audit, RNSW provided additional information concerning policies, procedures, processes, templates and training material relevant to its management of personal information under the PPIP Act. In its assessment the IPC relied on the material provided, information obtained in consultations with RNSW staff, as well as the data it assessed during the audit to inform its findings.

7.2 Assessment criteria

The IPC assessed RNSW's compliance with the PPIP Act against discrete criteria to reflect the issues identified. The criteria are set out in the table below.

Assessment criteria
PPIP delegations are in place
PPIP tools and systems are in place
PPIP culture and leadership is in place
PPIP governance processes are in place
PPIP training, support and communication is in place

7.3 Conduct of analysis

The findings of the review are presented in two parts:

- assessment against select criteria that assist examination of RNSW compliance with legislated requirements. The results of individual audit assessments provide objective findings and in some instances inform further findings or commentary.
- specific comments, findings and recommendations to assist RNSW with compliance with legislated requirements.

The IPC recorded and retained data in undertaking the audit. For the purposes of this report it was deemed not necessary to provide a breakdown as the findings and recommendations are applicable generally and not specifically.

8 Observations

8.1 PPIP delegations

Criterion		Result
a	Documented PPIP delegations are in place	Processes/procedures in place

Comments, findings and recommendations
Comment: Section 53(4) of the PPIP Act provides that an application under Part 5 – Review of certain conduct must be dealt with by an individual within the public sector agency who is directed to deal with the application. **Observations:** RNSW as part of the then DFSI cluster relied on DFSI for the exercise of corporate functions under section 53(4) of the PPIP Act. RNSW officers advised that the exercise of privacy functions under section 53(4) are within the scope of the corporate delegation functions. RNSW has an extensive suite of policies adopted from DFSI that are specific to particular functions and activities within the agency. These policies set out particular roles and responsibilities for staff across various functions within these policies. RNSW has a current form on its website - *Application for Review of the Conduct of Revenue NSW*. This form refers to DFSI. Consequent upon the machinery of government changes effective from 1 July 2019, DFSI ceased to exist and was assumed into DCS. Where RNSW relies on DCS to exercise corporate functions, such as review of conduct under Part 5 of the PPIP, RNSW should ensure that it is current and reflects machinery of government changes from DFSI to DCS. **Recommendation 1:** RNSW should review its corporate delegations to ensure that where it relies on DCS to exercise functions on its behalf, such as Part 5 of the PPIP Act, the corporate delegations are current and reflect machinery of government changes from DFSI to DCS. **Recommendation 2:** RNSW reviews its website content to update forms and information relevant to the operation of the PPIP Act and HRIP Acts to reflect the machinery of government changes from DFSI to DCS. **Recommendation 3:** Further to Recommendation 1, RNSW should review, with DCS, all of its policies relevant to privacy responsibilities to ensure that they accurately reflect changes from DFSI to DCS. Following review of these policies, RNSW should actively promote the location and circulate the updated policies to all staff.

8.2 PPIP Tool and Systems

Criterion		Result
a	Where personal information is stored	Processes/procedures not in place
b	What personal information is used for	Processes/procedures not in place
c	Who has access to personal information	Processes/procedures not in place
d	Processes to monitor that remediation actions have been followed and residual risks addressed	Processes/procedures in place
e	Processes for internal reporting to Senior Executive about potential breaches of privacy	Processes/procedures in place
f	Procedures in place to train staff on the policy and requirements	Processes/procedures in place

Criterion		Result
g	Undertakes corrective action to address root causes and non-compliance	Processes/procedures in place
h	Undertakes corrective action to address root causes and non-compliance	Processes/procedures in place
i	Documented processes	Not documented in all instances

Comments, findings and recommendations

Comment: While the PPIP Act does not stipulate that a privacy management or governance framework is required, it does stipulate that a privacy management plan (PMP) is required by each public sector agency.[11] A privacy management plan is a strategic planning document in which each public sector agency describes the measures it proposes to take to ensure that it complies with the PPIP Act and the HRIP Act.

A PMP provides

- the agency's policies and practices for complying with the PPIP Act and the HRIP Act
- how the agency will make its staff aware of these policies and practices
- the agency's procedures for dealing with privacy internal reviews under Part 5 of the PPIP Act
- other relevant matters relating to the protection of the personal and health information that the agency holds (section 33 of the PPIP Act).

A PMP is a useful reference point for staff and members of the public to inform and understand how the agency fulfils its requirements for compliance under the PPIP Act.

RNSW provided the IPC with a copy of the DFSI Privacy Governance Framework that it relies upon in the management of its privacy compliance. This is an internal document for the benefit of staff of the whole of the DFSI cluster.

Observations: RNSW has on its website a privacy statement (available from the Privacy Tab on its website)[12] which is distinguishable from a PMP. The privacy statement refers to the accessible pages on the RNSW website. The scope of the information included and required in a PMP is more extensive and particular. For the purposes of this audit, we reviewed RNSW website. We did not locate the equivalent of a PMP or a link to the PMP that may be the overarching PMP developed by DCS as part of its provision of corporate services. The IPC recognises that RNSW relies on DCS (previously DFSI) for the provision of corporate functions, however it is not easily apparent how RNSW fulfils the requirements of section 33 of the PPIP Act, enabling citizens to be able to easily identify the measures the agency has in place to comply with the legislation or how a citizen can exercise rights if necessary.

While a PMP was not identified nor a link to DFSI's PMP, the audit did identify that RNSW provided a

[11] Section 33 PPIP Act

[12] See https://www.revenue.nsw.gov.au/privacy

Comments, findings and recommendations
copy of its DFSI Privacy Governance Framework as at April 2019 as the processes and procedures relevant to its management of personal information. The observations that follow are a consideration of those internal processes/procedures. The IPC reviewed the procedural documents provided by RNSW at the audit and observed that RNSW relied on a DFSI Privacy Governance Framework (the Framework) to underpin its privacy practices within RNSW. The Framework states that it is intended to apply to all DFSI's Divisions and Related Entities and is an internal guideline for DFSI staff on how the principles and aims of the DFSI Privacy Management Plan are embedded in the Department's integrated policies, operating plans, business processes and work practices[13]. It is not in dispute that RNSW relies on the Framework in conjunction with other policies, the Framework is general in its application and does not adequately address the operating context for RNSW. The Framework includes and describes roles and responsibilities across the DFSI cluster, this includes at Secretary, Senior Executive, Management and individual staff level. While the Framework importantly articulates the roles and responsibilities and provides a whole of Department statement of commitment to privacy governance, it does not include a description of the specific types of personal information that is collected by RNSW. This is likely to be because the Framework is intended to be overarching and applicable across the numerous business divisions within the Department. Accordingly, in our consideration of the Framework we were not satisfied that it can be relied upon by RNSW in all aspects, because it does not contextualise the particular personal information that is collected within RNSW, where it is stored, how the information is used in the particular operating context of RNSW, or who has access to that information and the purposes for that access. Consideration was given to other supporting RNSW policies that were made available to identify whether this level of description around the collection of personal information is articulated in other policies that were provided. Additionally, consideration was given to the Personal Information Holding – Personal Information Inventory (PII) – that is included within the Framework which we understand is intended to be informed by self-assessment and is intended to understand the personal information holdings and how information is currently being held. However, it is not apparent from the Framework how this PII provides the necessary communication to all staff across all levels the types of personal information that is collected by RNSW, the purpose of the collection, storage and access. RNSW would benefit from developing a clear policy statement that addresses these requirements. RNSW informed us that the induction process includes RNSW Information Security training for all staff. We accept this occurs at induction. However, any training at induction would be supplemented by the development of this policy which is accessible outside of the induction process, the purpose of which is to ensure that at all levels there is clarity within the RNSW operating context. Additionally, mechanisms should be established for the regular review of the currency of the training content, in conjunction with a process for ongoing refresher training for staff at regular intervals. The Framework also includes specific requirements on privacy risk management, privacy breach management, evaluation, reporting and assurance. As part of the Framework, requirements are in place to provide for the internal reporting of incidents. This includes monthly divisional reporting, weekly executive reporting and quarterly reporting and analysis to the Audit and Risk Committee (ARC). This includes a post incident review. Our review of RNSW specific policies is dealt with in more detail in later parts of this report. **Recommendation 4:** RNSW engages with DCS to review its website to ensure that it fulfils and satisfies the requirements of section 33 of the PPIP Act.

[13] DFSI Privacy Governance Framework, April 2019 at page 8

Comments, findings and recommendations
Recommendation 5: RNSW engages with DCS in relation to its Privacy Governance Framework to reflect the application of the PPIP Act to its operating context. **Recommendation 6:** RNSW develop a clear policy statement that describes the types of personal information that it collects, the purposes of the use of that personal information and where personal information is stored and how it can be accessed, particular to the RNSW operating context. Once this is done, RNSW should take steps to include the policy in its training program and socialise the policy with staff. **Recommendation 7:** RNSW should develop a mechanism to ensure that its training content is regularly reviewed to ensure currency, and that there is in place a process for staff to undertake refresher training at regular intervals.

8.3 PPIP Governance for authorised disclosure of personal information

An effective privacy governance framework for the management and authorised disclosure enables sound and robust management of personal information. Having in place appropriate and adequate policies, processes and systems that are documented supports an agency in achieving privacy governance. The IPC website provides a number of resources available to agencies to support effective privacy governance, including template forms, a privacy governance framework, a self-assessment tool and data breach resources.

This audit was confined to the governance arrangements that RNSW had in place for the authorisation of disclosure of personal information only. For the purposes of the audit, it was accepted that the personal information collected was in accordance with the requirements of the PPIP Act.

Criterion		Result
a	A policy/procedure for information sharing outside of the agency	Processes/procedures in place
b	A system and process for communicating and training about the policy/procedure to all staff	Processes/procedures not in place
c	A process for reviewing and confirming that disclosure of the data is in accordance with policy/procedure	Processes/procedures in development
d	A process for confirming and approving that the disclosure is authorised	Processes/procedures in place
e	A delegation policy/ procedure authorising who can release of information	Processes/procedures in place
f	A process for auditing disclosures against the policy/procedure	Processes/procedures in place
g	A process of reporting compliance against the policy to Senior Executive	Processes/procedures in place
h	A framework for review of its policies and procedures	Processes/procedures in place
i	has a mandated governance structure and authorisation process for disclosure of information with other agencies	Processes/procedures in place

Comments, findings and recommendations
Comment: Section 18 of the PPIP Act sets out the limits on disclosure of personal information. Section 18 of the PPIP Act is to be read in conjunction with other provisions of the PPIP Act which provide for specific exemptions from the privacy principles, along with any public interest directions or codes of practice that may apply from time to time. At the time of the audit, there were no public interest directions or codes of practice on behalf of RNSW that modified the application of the IPPs by RNSW.[14] However, application of other exemptions provided for under the PPIP Act may have application in particular circumstances. The variable nature of the application of the specific exemptions from the privacy principles under the PPIP Act are such that this audit could not consider each applicable exemption because the application of the exemptions is to be considered having regard to the particular facts and circumstances. The observations and recommendations are therefore made in this context. **Observations:** RNSW has a Guidance Note *for Advice for the Release of Revenue NSW Data to External Parties*. This policy establishes data stewards as having responsibility for recommending release of RNSW data to external parties, with overall responsibility for approval sitting with RNSW Executive. Under the policy there is a requirement that all data must be approved for release by the relevant Revenue NSW Executive and applies a centralised coordination to the release of data. Significantly the policy includes that the data is to be quality assured to ensure that no personal or confidential information is included as a final step in the process. It may be implicitly intended in the process, however it is not without doubt, that the quality assurance process for the data set to be released occurs after the approval for release has occurred. Accordingly, it would assist if the policy includes at the point of the provision of the data for review and recommendation to the appropriate Executive Director, assurance that it is de-identified and does not include confidential or personal information. We note that the authorisation for approval to disclose information outside of the agency is at senior executive level. The guidance note also includes a mechanism for periodic audit to be undertaken on a quarterly basis of a random sample. The reports of which will be submitted to RNSW Executive enabling oversight at senior officer level. RNSW may wish to consider how this quarterly reporting will sit within the broader reporting to DCS as the Department. As the DCS has ultimate responsibility for the annual reporting for compliance under the PPIP Act for all business divisions, additional reporting on the outcomes from the periodic audit to DCS may be appropriate. At the time of the site visit, we understand that the first periodic audit was due to take place. As part of the delivery of services it is to be expected that government business units will receive and prepare correspondence either in response to, or on behalf of, their Minister. RNSW has a policy that outlines its process for doing so. Given the nature of the functions of RNSW it is likely that this correspondence may include personal information, such as in the case of a penalty notice. It is noted that the PPIP Act provides for an exemption[15] that is likely to be relevant to this process. There is no reference to the application of this exemption in the procedure. It may assist to address the application of the exemption to provide certainty with the procedure for those with a role and responsibility under the procedure relative to the broader privacy principles. In our review we were also provided with the RNSW's process document for media contact for information. This is a process document which by its nature has an external disclosure dimension outside of RNSW. For the purposes of this audit we reviewed the process document. It does not include in its initial review and discovery stage an explicit instruction or assessment in relation to review

[14] Section 41 PPIP Act

[15] Section 27A PPIP Act

Comments, findings and recommendations
whether the information requested seeks access to personal information. The process, given the potential scope of information that could be requested, should include a specific instruction about an assessment of the information request for personal information and how such a request should be handled, including by reference to other policies that also deal with personal information. Such instruction should have regard to the broader policies related to personal information referenced and recommended elsewhere in this report. RNSW also made available to the audit other policies that it uses to manage its business. While these were provided and considered, they were considered to more appropriately relate to how RNSW conducts its internal operations and business for the purposes of discharging its general functions in responding to other formal processes. In these circumstances, as it relates to its internal management as distinct from privacy, we have made no observations. Similarly, we were provided with a copy of its internal process for the MP Hotline. We reviewed this procedure from a privacy perspective, and we make no observations. This is because it similarly relates to the administrative processes RNSW has in place to respond to calls to the MP Hotline from members of Parliament and their staff for all matters relating to RNSW fines, taxes, duties, grants, benefits and unclaimed money. We have previously in this report observed an absence of an overarching policy that addresses the particulars of the personal information holdings, collection, use and storage and access for the RNSW operating context. Our view of the need for such an overall policy was confirmed in the review of the policies we considered for disclosure of information. The common theme across these policies was an absence of a discussion on the meaning of personal information in the context of the application of these policies. While it may be implicit, the consideration of the existing policies confirmed our view of the need for such policy to be developed. **Recommendation 8:** RNSW review its Guidance Note – Release of RNSW Data to External Sources – to include at the point of review and recommendation to the appropriate Executive Director assurance that the information is de-identified and does not include confidential or personal information. **Recommendation 9**: RNSW considers including in its Guidance Note a reporting requirement on the outcome of results from the periodic audit to the DCS. **Recommendation10:** RNSW considers reviewing its procedure for ministerial correspondence to address the application where relevant of any exemptions under the PPIP Act which may authorise non-compliance with the IPPs as appropriate to its legislative and operating context. **Recommendation 11:** RNSW reviews its media contact process within business units to include a review and assessment of the request for personal information. In doing so this should include instruction and direction as to how such information requests should be managed and directed appropriate to its legislative and operating context consistent with RNSW privacy policies and procedures

8.4 PPIP - Privacy breach management

Unlike other jurisdictions[16], NSW does not currently provide for a mandatory data breach notification scheme under the PPIP Act for unauthorised disclosure of personal information. At the time of this audit, it is noted that the NSW Department of Communities and Justice (DCJ) had released a discussion paper

[16] Currently the Commonwealth jurisdiction has a mandatory data breach scheme established by its mandatory data breach notification scheme.

on a Mandatory Data Breach Scheme for NSW.[17] That discussion paper remains the subject of an ongoing process.

Accordingly, the consideration of RNSW's data breach management is in the context of a voluntary scheme that is promoted and encouraged by the NSW Privacy Commissioner and not currently required under the PPIP Act.

Criterion		Result
a	A data breach policy that is understood by all staff	Processes/procedures in place
b	A data breach response plan	Processes/procedures in place
c	An identified data breach response team	Processes/procedures in place
d	A communications plan in the event of a breach	Processes/procedures in place
e	Processes in place to voluntarily notify the Privacy Commissioner	Processes/procedures in place
f	Processes to monitor to ensure that remediation actions have been followed and residual risks addressed	Processes/procedures in place

Comments, findings and recommendations
Comment: RNSW advised that it has a data breach policy and has made available to the IPC a copy of its Privacy Breach Management Process. At the time of the audit this process was in draft form. It is supplemented with a RNSW Privacy Breach Responsibilities document and Data Breach Log. The draft policy includes details on roles, responsibilities and instructions for staff on responding to an unauthorised disclosure of personal information. **Observations:** RNSW's draft Privacy Breach Management Process includes reference to other documents that are to be read in association with the policy. Having a centralised policy that deals with all relevant aspects would be more desirable and efficient, ensuring a comprehensive policy is in place. It would also ensure that there is no inconsistency between the Privacy Breach Management Process and other supporting documents. The Privacy Commissioner has released a data breach policy which provides some guidance to agencies which may inform the finalisation of RNSW's draft policy. RNSW's draft policy defines a privacy breach to mean *an unauthorised use of personal information as defined in the PPIP Act.* This appears to adopt a narrow construction of the definition of a privacy breach. However, a privacy breach is not limited to the use of personal information, which is generally considered to be conduct associated with inside an agency. A privacy breach is not limited to just a consideration of the IPP associated with use[18]. A privacy breach may arise as a consequence of a breach of any of the other IPPs, for example disclosure that is not authorised or permitted under the PPIP Act, or from a failure to adequately dispose of personal information securely.[19] The draft policy would benefit from a review of the definition of a data breach to ensure that it appropriately captures the

[17] https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/mandatory-data-breach-notification.aspx

[18] Section 17 PPIP Act

[19] The IPP's are dealt with in sections 8 – 19 of the PPIP Act.

Comments, findings and recommendations
scope of the conduct that may constitute a data breach. The policy does not consider the potential for privacy breaches arising from cyber security related instances such as malware, hacking, ransomware among others which may result in the compromise to personal information of RNSW customers. Accordingly, in any finalisation of the draft policy, RNSW should consider including any relationship with its cyber security management policy where privacy considerations are enlivened. The draft policy adopts a singular approach to personal information and does not distinguish between personal information of an individual and that which relates to information about an organisation such as a corporate entity. Given the scope of the customer base that interacts with RNSW, likely to be both individuals and corporate entities, the policy may benefit from inclusion of a definition of personal information and sensitive personal information in the context of the different customers that interact with RNSW. It is acknowledged that the policy includes the activation of a breach management team to respond and oversee the response. The activation of the response team includes the management of agreed actions required in response, including the record of breaches within its registers for both RNSW and DCS and post incident review. Timeframes are assigned to business rules for the completion of actions associated with the privacy breach. Supplementary to the draft policy is a document that details responsibilities across areas for Privacy breaches. Clearly setting out the responsibilities for privacy breaches assists to ensure that the responsibilities for privacy are clear and understood. The utility in having a separate and distinct document however, is unclear. Having a single, comprehensive policy process that addresses all aspects relevant to privacy breaches would seem to be on the face of it, an efficient and effective approach to embedding the requirements and expectations within RNSW. The audit noted that the supplementary document also references Responsibilities for the Privacy Contact Officer. It is not readily apparent whether that this is a reference to a role that is within RNSW or DCS or both. Similarly, reference is also made to the Revenue NSW Principal Policy Officer. However, given the scope of RNSW it would appear that there is likely to be a Principal Policy Officer assigned to different functional areas within RNSW. The finalisation of the draft policy should consider consolidation of all relevant processes into a single document and address with particularity the relevant roles assigned to each responsibility to eliminate any potential for misunderstanding. During the course of the audit, officers for RNSW informed the IPC that it is intended to deliver further training to staff on its privacy breach process. Further training to support staff in their responsibilities and compliance with the agency's process will further embed the importance placed organisationally on privacy such that requirements and operations remain visible and transparent, to users and providers alike. Both policies make provision for the responsibility for notification to customers relevant to where a privacy breach has occurred. However, it is not clear whether the policy intends that in every instance a notification is to occur or only where an assessment of a breach causing serious harm has been assessed. Accordingly, if a risk assessment approach is applied, the policy would benefit from its inclusion into the process. The internal policy includes business rules that apply to direct the timeframes of actions that are to be taken. It is noted that this does not include a timeframe for notification to individuals affected by the breach. RNSW should address this business requirement to minimise any confusion over the timing of notification and to ensure that the timing enables an individual affected to act in their interests to minimise any harm or risk of harm arising from the breach. RNSW may wish to consider such timeframes against its risk assessment framework applied to the data breach process. Part of the internal process includes the escalation and notification to Senior Officers, including at

Comments, findings and recommendations
Deputy Secretary level concerning any privacy breach which has occurred. The notifications are then included in the register of notifications which have been occurred. Officers explained during the audit that the oversight for the remediation of actions by RNSW is overseen by the Risk and Assurance Team. The register we were provided with and reviewed demonstrated that recording of breaches was included. While inclusion of the requirement to include the information in the register is captured within the policy, the policy framework does not include ongoing reporting about the remediation of the breaches to Senior Officers, the number of complaints received in response or actions/advice taken in response to a Privacy Commissioner notification. Additionally, it does not address where responsibilities lie to implement any actions or advice suggested by the Privacy Commissioner arising from a notification made, including arrangements that ensure oversight at senior levels further promotes a proactive orientation to the prevention of privacy breaches through building the protection of personal information into standard practices, systems and operating procedures at all levels[20]. We understand that reporting forms part of the monthly report and is part of the risk and privacy report to the Ops Board (executive committee) monthly. RNSW should include in its policy internal reporting requirements to Senior Officers of privacy breaches on at least a quarterly basis. The report should include actions taken in response to advice suggested by the Privacy Commissioner, including where a decision is not made to adopt such advice. **Recommendation 12**: RNSW to review its draft Privacy Breach Management Process to include all relevant and associated documents, creating a single and comprehensive policy document for the management of privacy breaches. RNSW in finalising its draft Privacy Breach Management Process consolidates all relevant processes into the process, including addressing the particularity of roles and responsibilities as appropriate to DCS, RNSW and functional areas. **Recommendation 13**: RNSW in finalising its draft Privacy Breach Management Process should include a risk assessment model for the categorisation and escalation of privacy breaches if such is applied to when notifications to affected persons will or will not be made. **Recommendation 14:** RNSW should include in the Privacy Breach Management Process the procedures for managing cyber security breaches where they involve personal information. **Recommendation 15:** The draft policy is reviewed to include a definition of a data breach that appropriately captures the scope of the conduct that may constitute a privacy breach. **Recommendation 16**: That the draft policy include a definition of personal information that captures the different types of customers that interact with RNSW. **Recommendation 17**: RNSW should include in its policy internal reporting requirements to report privacy breaches to Senior Officers on at least a quarterly basis, including the number of breach notifications notified to the Privacy Commissioner. The report should include actions taken in response to advice suggested by the Privacy Commissioner, including where a decision is made to not adopt such advice, and the reasons for not doing so, and the number of internal reviews/complaints received as a direct response to the data breach. **Recommendation 18:** RNSW reviews its policies to include timeframes for the notification to individuals of a privacy breach by RNSW.

[20] Privacy Governance Framework at https://www.ipc.nsw.gov.au/sites/default/files/file_manager/PC_Foreword_FINAL.pdf

8.5 PPIP training, support and communication

The audit results reflect information obtained at the time of conducting the audit.

Criterion		Result
a	An established training program for all staff about privacy requirements and responsibilities	In place
b	A training program which is mandatory for all staff that addresses privacy requirements and responsibilities	In place
c	A program to induct all new employees about the handling of personal information under the PPIP Act	In place
d	Has a mechanism to ensure refresher training is available to all staff about privacy	In development
e	Delivered training on privacy to staff in the last 12 months	In place
f	Has a mechanism to confirm training is completed by all staff	In place
g	A documented training program	In place
h	A documented training register/record	In Place

Comments, findings and recommendations
Comment: RNSW at the time of the audit was in the process of delivering further privacy training for all staff within its Agency. All RNSW staff are required to complete mandatory Introduction to Privacy training which is completed by way of an e-learning package. The training package was developed by DFSI as the cluster agency. The training provides staff with an introduction to the PPIP Act, the IPPs and responsibilities and concludes with a brief assessment. Core privacy training is required to be completed by all RNSW staff. The Agency utilises a centralised system for recording training attendance and completion. Training completion records are reviewed and where appropriate, non-completion is followed up directly with staff concerned, including direct communications at Commissioner level to staff. The training records provided demonstrated the privacy training completion rates for three periods in the month of May according to the group functions within RNSW. The completion record as at 13 June 2019 showed that over the three periods the completion rates increased and ranged from between 81% to 100% completion. The Agency informed us that the completion of the training followed promotion of communication by the Agency at Deputy Secretary level in its newsletter of the need to complete the privacy training. The Agency promotes a privacy culture within the Agency through the use of regular communications with staff that includes weekly tips and “Brady’s Buzz”, an internal newsletter addressing the importance of privacy and requirements for training to be completed. At the time of the audit the delivery of training was completed under DFSI. RNSW was revisiting the training arrangements with DCS for additional or new requirements going forward.

Comments, findings and recommendations
Observations: RNSW has in place core foundation privacy training that is required to be completed by all staff across RNSW. Systems are in place to monitor the completion of training and where appropriate targeted follow up is in place. At the time of the audit, the IPC understands that RNSW has a mechanism to ensure refresher training is available to all staff about privacy under development. The importance of continued training is a key element to ensuring that there is a strong privacy culture. The e-learning training module is extensive and provides relevant general information for staff. The training is provided to staff to understand and meet their responsibilities in management of personal information and disclosure. However, because of their role and functions within the Agency particular staff, have specific responsibilities relevant to privacy arising from the application of specific functional policies that are in place. Roles and responsibilities are defined within these particular policies. Given the heightened privacy responsibilities for these staff, whether related to the collection, use or disclosure of personal information, staff may benefit from more targeted and specific training that is contextualised to these roles and responsibilities outlined in the functional policies and to the types of personal information handled by RNSW. **Recommendation 19**: RNSW is to review and consider application of targeted and specific training that is contextualised to the functional policies in place with focus on the privacy aspects of these roles and responsibilities specific to RNSW staff. RNSW finalise and implement its mechanism to ensure refresher training is available to all staff.

9 Conclusions and recommendations

9.1 Conclusions

This audit was informed by:

- a voluntary data breach notification
- media reports relevant to the events surrounding the voluntary data breach
- RNSW data provided as a consequence of the audit
- information obtained during the course of the audit.

In summary, this audit has identified:

- a high level of engagement with the PPIP Act and active promotion of its purpose
- an established training program for all staff with high completion rates
- a commitment at senior levels to ensure training completion
- defined roles and responsibilities relevant for some privacy related functions
- opportunities to improve processes to support compliance in respect of data breach and privacy governance requirements.

9.2 Recommendations

Based on the findings of this audit, it is recommended that RNSW implement the following within the timeframes specified:

Recommendations	
Recommendation 1:	RNSW should review its corporate delegations to ensure that where it relies on DCS to exercise functions on its behalf, such as Part 5 of the PPIP Act, that a formal authorisation addressing the specific decision-making responsibilities and functions to be exercised is in place. That review should ensure that the corporate delegations are current and reflect machinery of government changes from DFSI to DCS.
Recommendation 2:	RNSW reviews its website content to update forms and information relevant to the operation of the PPIP Act and HRIP Act to reflect the machinery of government changes from DFSI to DCS.
Recommendation 3:	Further to Recommendation 1, RNSW should review with DCS all of its policies relevant to privacy responsibilities to ensure that they accurately reflect changes from DFSI to DCS. Following review of these policies, RNSW should actively promote the location and circulate the updated policies to all staff.
Recommendation 4	RNSW engages with DCS to review its website to ensure that it fulfils and satisfies the requirements of section 33 of the PPIP Act.
Recommendation 5	RNSW engages with DCS in relation to its Privacy Governance Framework to reflect the application of the PPIP Act to its operating context.
Recommendation 6	RNSW develops a clear policy statement that describes the types of personal information that it collects, the purposes of the use of that personal information, where personal information is stored and how it can be accessed particular to the RNSW operating context. Once this is done RNSW should take steps to include the policy into its training program and socialise the policy with staff.
Recommendation 7:	RNSW should develop a mechanism to ensure that its training content is regularly reviewed to ensure currency, and that there is in place a process for staff to undertake refresher training at regular intervals.
Recommendation 8	RNSW review its *Guidance Note – Release of RNSW Data to External Sources* to include at the point of review, and recommendation to the appropriate Executive Director, assurance that the information is de-identified and does not include confidential or personal information.
Recommendation 9	RNSW considers including in its Guidance Note a reporting requirement on the outcome of results from the periodic audit to the DCS.
Recommendation 10	RNSW considers reviewing its procedure for ministerial correspondence to address the application where relevant of any exemptions under the PPIP Act which may authorise non-compliance with the IPPs as appropriate to its legislative and operating context.
Recommendation 11	RNSW reviews its media contact process within business units to include a review and assessment of the request for personal information. In doing so this should include instruction and direction as to how such information requests should be managed and directed appropriate to its legislative and operating context consistent with RNSW privacy policies and procedures.

Recommendations	
Recommendation 12	RNSW to review its draft Privacy Breach Management Process to include all relevant and associated documents, creating a single and comprehensive policy document for the management of privacy breaches. RNSW, in finalising its draft Privacy Breach Management Process, consolidates all relevant processes into the process, including addressing the particularity of roles and responsibilities as appropriate to DCS, RNSW and functional areas.
Recommendation 13	RNSW, in finalising its draft Privacy Breach Management Process, should include a risk assessment model for the categorisation and escalation of privacy breaches if such is applied to when notifications to affected persons will, or will not, be made.
Recommendation 14	RNSW should include in the Privacy Breach Management Process the procedures for managing cyber security breaches where they involve personal information.
Recommendation 15	The draft policy is reviewed to include a definition of a data breach that appropriately captures the scope of the conduct that may constitute a privacy breach.
Recommendation 16	That the draft policy include a definition of personal information that captures the different types of customers that interact with RNSW.
Recommendation 17	RNSW should include in its policy internal reporting requirements to report privacy breaches to Senior Officers on at least a quarterly basis, including the number of breach notifications notified to the Privacy Commissioner. The report should include actions taken in response to advice suggested by the Privacy Commissioner, including where a decision is made to not adopt such advice, the reasons for not doing so and the number of internal reviews/complaints received as a direct response to the data breach.
Recommendation 18	RNSW reviews its policies to include timeframes for the notification to individuals of a privacy breach by RNSW.
Recommendation 19	RNSW is to review and consider application of targeted and specific training that is contextualised to the functional policies in place with focus on the privacy aspects of these roles and responsibilities specific to RNSW staff. RNSW finalise and implement its mechanism to ensure refresher training is available to all staff.
Recommendation 20	RNSW report back regarding implementation of the recommendation within this report to the Privacy Commissioner by 1 May 2020.

9.3 Monitoring

The IPC will continue to assist RNSW as it adopts these recommendations and requests a report back regarding implementation by 1 May 2020.

10 Audit chronology

Date	Event
6 June 2019	IPC Notification to Revenue NSW in accordance with section 36 of the PPIP Act (requesting commencement in late June 2019)
13 June 2019	Correspondence from Revenue NSW responding to IPC notification
25 June 2019 inclusive	Conduct of onsite audit by IPC
10 July 2019	Provision of additional information by Revenue NSW
10 July 2019	IPC Request for additional information from Revenue NSW
22 July 2019	Response to IPC by Revenue NSW of additional information request
3 December 2019	Provision of draft report Revenue NSW
8 January 2020	Receipt of RNSW Response to Draft Report
31 March 2020	Provision of final report to the Revenue NSW

11 Legislation

The following legislation is relevant to the conduct of this audit.

Privacy and Personal Information Protection Act 1998 – relevant sections

- Part 2 – Division 1 – Information protection principles
- Section 33 – Privacy Management Plans
- Section 36 – Functions of the Privacy Commissioner
- Section 39 – General procedure for inquiries and investigations

12 Appendix A

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Protection Act 1998* (PPIP Act). The information outlined below is to be used as a guide only. A full text of the Information Protection Principles can be found in the relevant sections of the PPIP Act.

12.1 General Information

There are legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information. As exemptions may apply in some instances, it is therefore suggested you contact the Privacy Contact Officer in your agency or our office for further advice.

12.2 Collection

1. Lawful

Only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.

2. Direct

Only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.

3. Open

Inform the person you are collecting the information from why you are collecting it, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.

4. Relevant

Ensure that the personal information is relevant, accurate, complete, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

12.3 Storage

5. Secure

Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

12.4 Access and Accuracy

6. Transparent

Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

7. Accessible

Allow people to access their personal information without excessive delay or expense.

8. Correct

Allow people to update, correct or amend their personal information where necessary.

12.5 Use

9. Accurate

Make sure that the personal information is relevant, accurate, up to date and complete before using it.

10. Limited

Only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

12.6 Disclosure

11. Restricted

Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded

An agency cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

13 Appendix B

The 15 Health Privacy Principles (HPPs) are the key to the *Health Records and Information Privacy Act 2002* (HRIP Act).

These are legal obligations which NSW public sector agencies and private sector organisations must abide by when they collect, hold, use and disclose a person's health information. Exemptions may apply, therefore it is suggested you contact the Privacy Contact Officer or the Health Information Manager in the organisation or agency in the first instance. Or contact the Information and Privacy Commission NSW (IPC) for further advice.

13.1 Collection

1. Lawful

An agency or organisation can only collect your health information for a lawful purpose. It must also be directly related to the agency or organisation's activities and necessary for that purpose.

2. Relevant

An agency or organisation must ensure that your health information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

3. Direct

An agency or organisation must collect your health information directly from you, unless it is unreasonable or impracticable to do so.

4. Open

An agency or organisation must inform you of why your health information is being collected, what will be done with it and who else might access it. You must also be told how you can access and correct your health information, and any consequences if you decide not to provide it.

13.2 Storage

5. Secure

An agency or organisation must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

13.3 Access and accuracy

6. Transparent

An agency or organisation must provide you with details regarding the health information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency or organisation must allow you to access your health information without unreasonable delay or expense.

8. Correct

Allows a person to update, correct or amend their personal information where necessary.

9. Accurate

Ensures that the health information is relevant and accurate before being used.

13.4 Use

10. Limited

An agency or organisation can only use your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 10 applies). Otherwise separate consent is required.

13.5 Disclosure

11. Limited

An agency or organisation can only disclose your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 11 applies). Otherwise separate consent is required.

13.6 Identifiers and anonymity

12. Not identified

An agency or organisation can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.

13. Anonymous

Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

13.7 Transferrals and linkage

14. Controlled

Only transfer health information outside New South Wales in accordance with HPP 14.

15. Authorised

Only use health records linkage systems if the person has provided or expressed their consent.