

PRIVACY COMMISSIONER

Annual Report 2023



Annual Report of the Privacy Commissioner

for the year ended 30 June 2023

Presented to the House of Representatives pursuant to section 150 of the
Crown Entities Act 2004.

The Minister of Justice

I tender my report as Privacy Commissioner for the year ended 30 June 2023.



M Webster
Privacy Commissioner
31 October 2023

Introduction Kupu Whakataki	2
Meet our leadership team	5
Privacy in Aotearoa New Zealand – the year in numbers Te Mana Matatapu i Aotearoa – te tau me ōna tino tau	7
Strategic objectives progress Te kauneke ki ngā whāinga rautaki	8
Objective 1: Privacy protection is effective and easy to achieve	8
Objective 2: Costs of privacy compliance are minimised	12
Objective 3: We are trusted as a fair and responsive regulator	15
Objective 4: We influence privacy practices and behaviour	19
Office and functions Te Tari me āna mahi	23
Independence and competing interests	24
Reporting	24
Staff	25
Statutory remuneration disclosures	26
EEO profile	27
Finance and performance report Pūrongo whakahaere pūtea me ngā tutukitanga	30
Statement of responsibility	31
Statement of performance	32
Impact of Natural Disasters and COVID-19 on performance	33
PBE FRS 48 service performance reporting	34
Statement specifying comprehensive income	35
Cost of service statement	36
Primary activity 1: Strategy and insights	38
Primary activity 2: Communications and education	39
Primary activity 3: Compliance and enforcement	40
Primary activity 4: Advice and advocacy	41
Primary activity 5: Investigations and dispute resolution	42
Statement of accounting policies	43
Statement of comprehensive revenue and expenses	45
Statement of changes in equity	46
Statement of financial position	47
Statement of cash flows	48
Notes to the financial statements	49
Appendices Ngā Tāpiritanga	64
Appendix A Processes and services	65
Appendix B	67
Appendix C Independent Auditor’s Report	80

Introduction | Kupu Whakataki

I orea te tuatara ka patu ki waho


E ngā mana, e ngā reo, e ngā rau rangatira,
tēnā koutou, tēnā koutou katoa
Ko Rangitikei te whenua tupu
Ko Tāmaki Makaurau te kāinga
Kei Te Whanganui-a-Tara au e mahi ana
Ko ahau te Kōmihana Matatapu
Ko Michael Webster ahau
Tēnā koutou katoa

Privacy is fundamentally about people and that's what's driven many of the achievements of the Office of the Privacy Commissioner this year: the desire to create a safe, regulated, and relevant privacy landscape for Aotearoa New Zealand.

This year we've worked hard to minimise the privacy harms that New Zealanders experience, and to push agencies to ensure privacy is as much a core business focus for them as health and safety or regular financial reporting. The work of our Investigations and Dispute Resolution team and our Compliance and Enforcement team is crucial to this mahi.

I've chosen to open my report with the above whakatauki, because it really speaks strongly to me of the enthusiasm with which the Office continues to find solutions to increasingly complex privacy problems. This year we've tackled emerging and increasingly topical privacy issues such as generative artificial intelligence (AI), biometrics, and children's privacy. We've been nimble, adaptive, and forward-looking in how we've tackled new challenges, engaged with New Zealanders, and established project teams to work on complex and future-focused privacy issues.





My Office continues to record an increase in privacy-breach notifications and complaints about data security, which affect agencies (businesses and organisations) as well as individuals. We need to ensure agencies know how to do privacy well, and educate them when they don't, and to use the enforcement tools at our disposal to increase compliance. We need the right people to do that work, and the funding we received in Budget 2023 has helped us to employ them.

Our team grew in number so that we could adapt to new and evolving challenges and continue the work of policy development, compliance, education, and resolution during a period of rapid technological development.


That technological development has highlighted once again that New Zealand's privacy law must be fit for purpose if it's to meet the challenges of the digital age. The legislative requirements and regulatory tools of the Privacy Act 2020 need to respond to the challenges of more and more complex data leaks, rising cyber-attacks, the increasing use of technologies like facial recognition, and the increasingly intensive data-processing power that tools like AI offer.

Overseas, most notably in our neighbour Australia, we've seen reforms aimed at strengthening penalties that strike at the pockets of privacy law violators. This year I wrote and spoke publicly about the need for the New Zealand Privacy Act to have a fit-for-purpose penalty regime. Such a regime would better incentivise the proper management of personal information by agencies, whether they're in the private, public, or not-for-profit sectors.

The Office will continue to ready New Zealand for a more challenging future. We look forward to developing its services and continuing to support New Zealanders, particularly those most vulnerable to privacy harm.

Michael Webster
Privacy Commissioner

We need to ensure agencies know how to do privacy well, and educate them when they don't, and to use the enforcement tools at our disposal to increase compliance.



Meet our leadership team

Privacy is fundamentally about people, and the people who lead the Office of the Privacy Commissioner (OPC) are passionate about that. We lead with people at our heart and have a commitment to Te Ao Māori.

Liz MacPherson Deputy Privacy Commissioner

Liz was appointed as the first statutory Deputy Privacy Commissioner in November 2021. She oversees the compliance, investigations and dispute resolution, and guidance and capability-building functions of OPC.

Tena koutou katoa
I whanau mai au i Tāmaki Makaurau
Nō Aerana, Kōtirana, Ingarangi me
Haina ahau
I tupu ake au i Puni, Tokirima, Waiuku,
Waiotira, Te Akau me Waimauku
Kei te Whanganui-a-tara tōku kāinga ināiane
Ko te Komihana Tuarua ahau
Ko Liz MacPherson tōku ingoa

Emma Boddy General Manager

Emma manages all our corporate service functions including HR, IT, finance, strategic and business planning, compliance reporting, and records management.

Tēna koutou katoa
Nō Ingarangi me Kōtirana ahau
I tipu ake ahau i Kōtirana
Kei Tāmaki Makaurau tōku kāinga
Ko Emma Boddy ahau

Peter Mee Assistant Commissioner, Strategy, Policy and Engagement

Peter's group includes the regulatory policy, communications and engagement, strategy, and Pou Ārahi teams at OPC.

Tēna koutou katoa
Nō te Wai Pounamu, nō Hakatere ahau
Kei Waikanae ahau e noho ana ināiane
Ko Peter Mee ahau
Tēna koutou katoa

Joanna Hayward General Counsel

Joanna is responsible for providing advice on law reform, legal assurance and compliance to the Privacy Commissioner, and legal representation on behalf of the Commissioner.

Tēna koutou katoa
Nō Ingarangi me Kōtirana ahau
Engari i tupu ake au ki te Waipounamu
Kei te Whanganui-a-tara tōku kāinga ināiane
Ko te Roia Matua au ki Te Komihana o te Mana
Mātāpono Matatapu
Ko Joanna Hayward ahau.

Acknowledgment of service

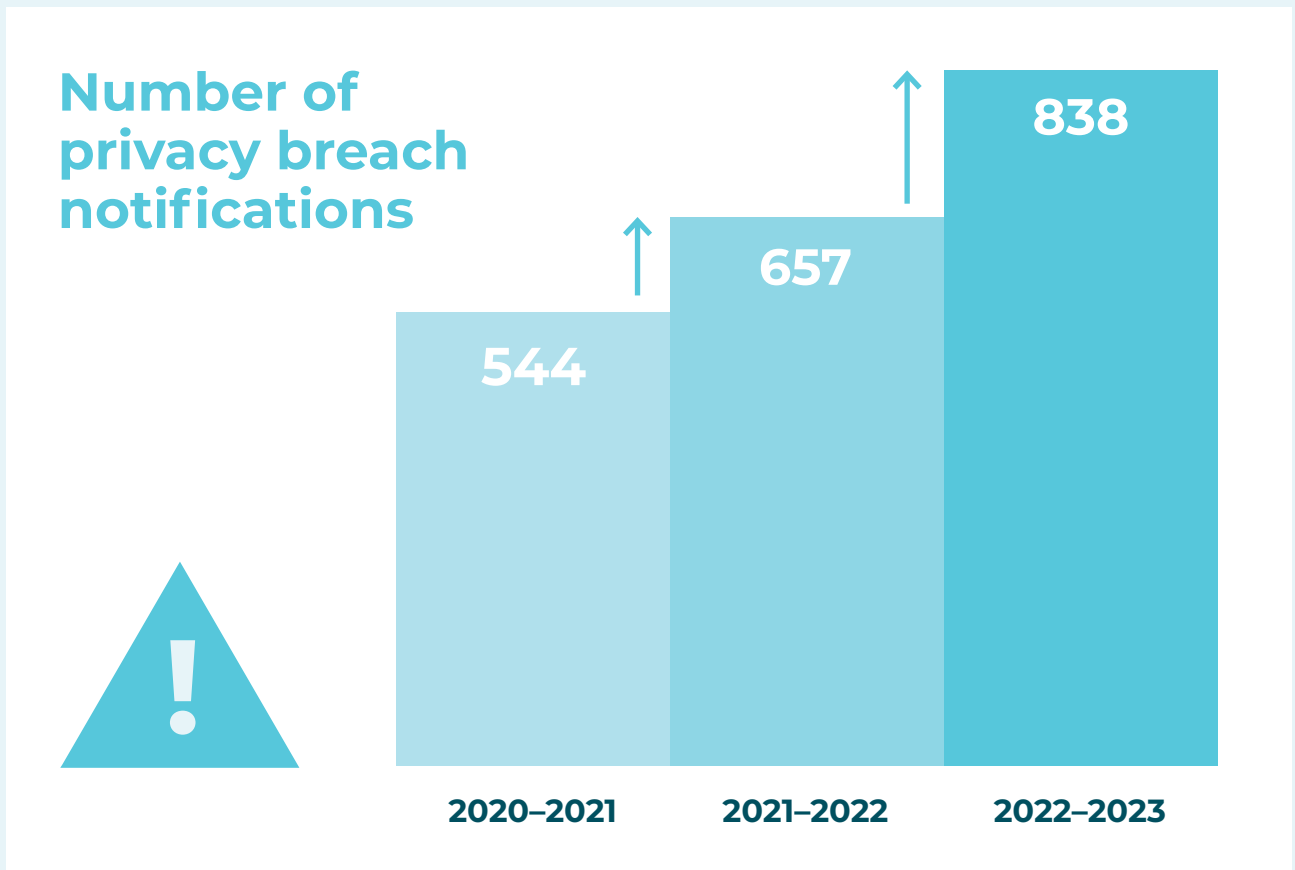
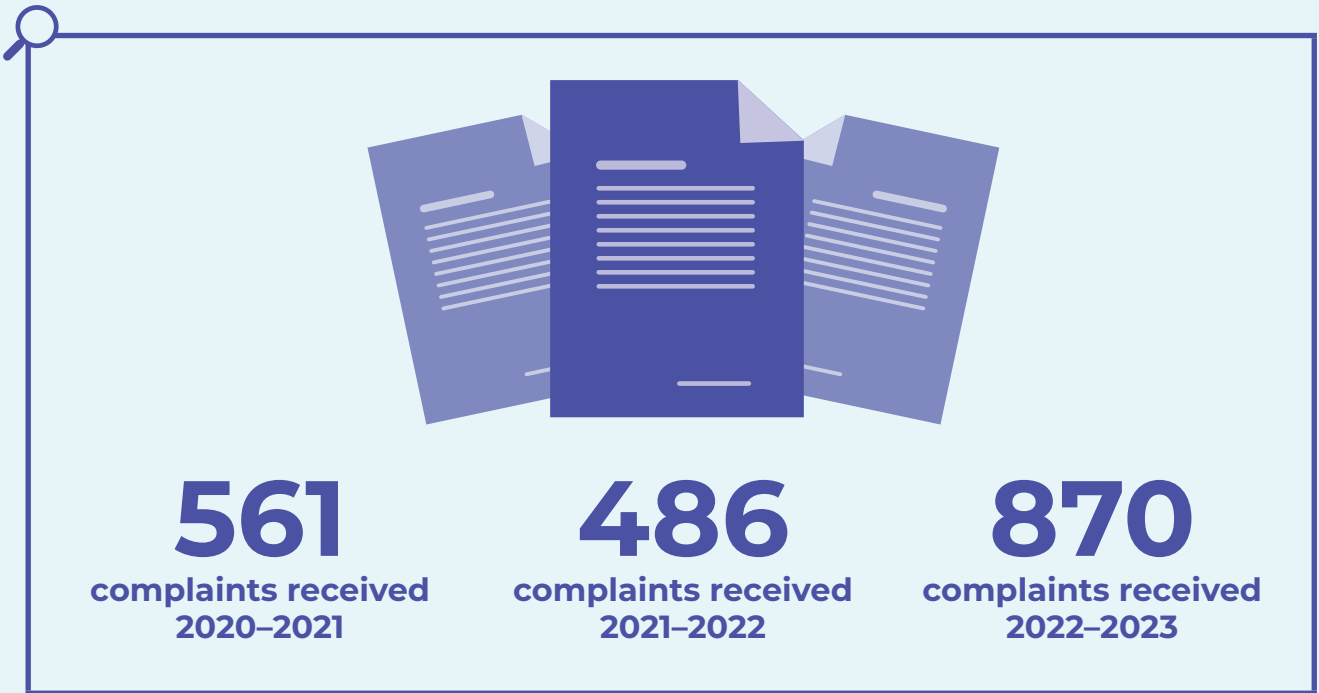
Gary Bulog, General Manager 1997-2023



Tēna Koutou
Nō Koroātia ahau
Nō Tāmaki Makaurau ahau
I tipu ake au ki raro i te maru o
Waitākere i te taha o te Waitematā.
Ko Gary Bulog ahau
Tēna koutou

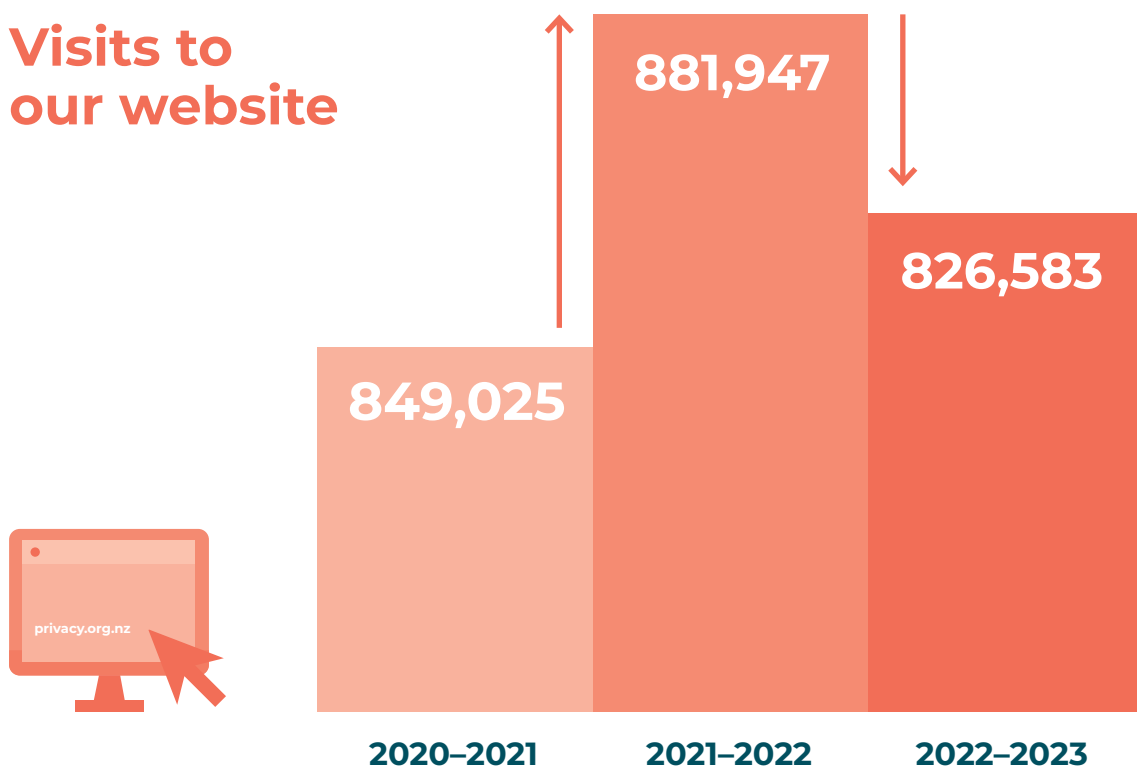
The Office wishes to say thank you to our retiring General Manager Gary Bulog for his tremendous contribution to OPC and the legacy he leaves behind. Gary managed all the Office's corporate service functions, including HR, IT and finance.

Privacy in Aotearoa New Zealand – the year in numbers | Te Mana Matatapu i Aotearoa – te tau me ōna tino tau





Visits to our website



Strategic objectives progress | Te kauneke ki ngā whāinga rautaki



Objective 1 | Whāinga 1 Privacy protection is effective and easy to achieve He whaikiko he māmā hoki te tutuki i te tiakitanga matatapu

Effective privacy protection means people can feel confident in the knowledge that organisations trusted with their personal information are equipped to safeguard it from harm.

When agencies and businesses put privacy at the heart of how their organisations operate, they build trust with their clients, patients, and customers. It's why we often say that privacy should be as important to businesses as health and safety or regular financial reporting.

Part of our role is to help people to respond well when a breach occurs. We support people and agencies with this, so they know what their obligations are and what they need to do to remedy any adverse situation.

At the end of 2022 we ran a Small Business Privacy Awareness Survey, and 386 small businesses responded. We took the results of that survey and added insights from 1487 breach reports to our Office to draw insights about small businesses and privacy. Our *What New Zealand small businesses can learn about privacy* (May 2023) Insights Report raised awareness in the small business sector of what good privacy policies and practices are, which was something we'd learnt through the survey that many businesses didn't have.

This year we invested in further developing our Compliance and Enforcement team. This team helps ensure that businesses and organisations comply with their privacy obligations under the Privacy Act 2020 (the Privacy Act). The team leads a range of compliance activities and investigations,

covering matters ranging from education to advice, compliance monitoring, risk management, and enforcement.

We aim to be nimble and knowledgeable in our work and constantly assess the privacy landscape to understand where we can best focus that work for maximum effect. The use of generative artificial intelligence (AI) as a work tool really took off this year, with chatbots, content creators, and transcription and meeting assistants all becoming very popular, very quickly. AI has been widely talked about as increasingly attractive, but it carries significant privacy risk, which the Commissioner noted in his opinion piece for media, *AI and privacy concerns go hand in hand*, in April 2023.

On 25 May 2023 the Privacy Commissioner outlined his expectations around AI use, issuing guidance to agencies and promoting it through media channels. This was an important step to ensuring AI tools are used in privacy-protective ways, consistent with the Privacy Act.

"I would expect all agencies using systems that can take the personal information of New Zealanders to create new content to be thinking about the consequences of using generative AI before they start," he said.



CASE STUDY ONE

We announced a joint investigation into Latitude Financial with our Australian counterpart

Latitude Financial formally notified us on 16 March 2023 that it had had a privacy breach as the result of a cyber-attack. Eventually we'd learn it was New Zealand's worst known privacy data breach and that it had exposed millions of New Zealanders' and Australians' records.

Across the two countries 14 million records were stolen, and of those 6.1 million were over 10 years old. Some records were at least 18 years old. They included drivers' licences, passports, and sensitive financial data such as personal income and expense information.

We announced a joint compliance investigation between OPC and the Office of the Australian Information Commissioner on 10 May 2023. A compliance investigation enables us to use our full information-gathering powers and includes our being able to oblige people to provide information, and to summon witnesses.

The investigation, which is ongoing, focuses on whether Latitude took reasonable steps to protect the personal information it held from misuse, interference, loss,

unauthorised access, modification, or disclosure. It's also considering whether Latitude took appropriate steps to destroy or de-identify personal information that it no longer required.

What the case has highlighted so far is a risk in the data-retention policies and practices of private and public agencies. Agencies should not be collecting or retaining personal information unless it's necessary for lawful purposes connected with their functions or activities. This is also just good business, because you can't have hacked what you've already deleted or what you've never collected in the first place.





CASE STUDY TWO

The Commissioner set his expectations on generative AI use

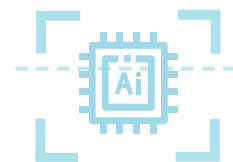
Privacy Commissioner Michael Webster issued his expectations on generative AI use on 25 May 2023 (and updated them on 15 June 2023).

In his role as regulator of New Zealanders' personal information, he called for businesses and organisations to check their obligations around generative AI use before they began using it. He made eight points to guide decision-makers in using the evolving technology.

OPC expects that any agency considering implementing a generative AI tool will:

1. Ensure that senior leadership has given full consideration to the risks and mitigations of adopting a generative AI tool and explicitly approved its use.
2. Review whether a generative AI tool is necessary and proportionate.
3. Only use a generative AI tool after conducting a privacy impact assessment (and/or algorithmic impact assessment) to help identify and mitigate privacy and wider risks.
4. Be transparent with customers and clients about how, when, and why the generative AI tool is being used and how potential privacy risks are being addressed.
5. Engage with Māori on the potential impacts of the generative AI tool on their communities and taonga.
6. If the generative AI tool will involve the collection of personal information of customers or clients, develop procedures for how the agency will take reasonable steps to ensure that the information is accurate before use or disclosure and for responding to requests from individuals to access and correct their personal information.
7. Ensure a review by a person prior to acting to detect inaccurate or biased information.
8. Ensure that personal or confidential information is not retained or disclosed by the generative AI tool.

It's clear that our country needs to directly address the opportunities and risks of generative AI.





CASE STUDY THREE

Hundreds and thousands: the IDR story

When New Zealanders experience privacy breaches, or agencies need to better understand how the Privacy Act applies to them, it's our Investigations and Dispute Resolution (IDR) team they contact.

Each year IDR handles hundreds of complaints and thousands of enquiries. In 2022-2023 there were 870 complaints and 6604 enquiries.

IDR runs a streamlined, structured process with people at its heart. This year it introduced a service charter that sets out what people can expect from the complaints process. It's guided by four principles: fairness, accessibility, responsiveness, and efficiency. It also explains the kind of behaviour we expect from people using our services.

How IDR investigates complaints

- If the team decides to investigate, it determines which principles of the Privacy Act may have been breached and how. It notifies the complainant and the agency involved that it's investigating the complaint.
- IDR conducts investigations by talking to the parties in person and by telephone, email, and letter. It may also ask a complainant to meet with the agency to discuss the complaint.

It might ask the complainant and the agency to provide documents and information relevant to the complaint, but won't pass on any correspondence between the parties. Both parties need to be able to speak to OPC openly for our investigation to be effective.

- During an investigation, IDR can form a view on whether the agency's actions have interfered with the complainant's privacy under the Privacy Act. If it forms a view against a group, IDR will give that party the chance to respond. We do this to help the parties understand how OPC sees the complaint, and to help people work towards a solution.
- The IDR team doesn't usually make legally binding rulings or determinations. However, its view is an important indication of whether there's been an interference with a person's privacy. The team closes most investigations within six months, but they can take longer depending on the individual circumstances.

Under Principle 6 of the Privacy Act, IDR can make enforceable determinations on access complaints.



Objective 2 | Whāinga 2

Costs of privacy compliance are minimised

Ka whakahekea ngā utu mō te whakaū matatapu

By enabling organisations to reach levels of privacy maturity, we help them to identify ways to manage their collection and use of people's personal information and comply with the Privacy Act.

Our research shows that Māori communities are at risk of harm from privacy breaches, which is why nurturing relationships, understanding Te Ao Māori ourselves, and ensuring Māori groups are part of our engagement work are so important.

When we launched a consultation paper on the regulation of biometrics in August 2022, we knew the voices of Māori would be important because of the tapu nature of biometrics. We heard from Māori that biometric information is related to whakapapa and carries the mauri of the individual from which it was taken.

Work has continued on biometrics, alongside AI and children's privacy, and a consideration of Te Ao Māori has been included at each stage.

By working alongside Māori and increasing our staff's capabilities in this area, we expect to see an increase in privacy education across the wider community. We've identified Māori as a group that's at risk of privacy breaches. Our work here is expected to help mitigate privacy harm in this group in the future.

This year we also completed work with whānau Māori and the Independent Police Conduct Authority on a joint report on Police photographing rangatahi Māori.

By working alongside Māori and increasing our staff's capabilities in this area, we expect to see an increase in privacy education across the wider community.





CASE STUDY ONE

Focusing our kaupapa on mahi tahi

*Nāu te rourou, nāku te rourou,
ka ora ai te iwi*

*With your food basket and my food
basket, the people will thrive*

Acknowledging the Treaty of Waitangi and incorporating a Te Ao Māori perspective has helped our Office to strengthen our work practices and work with our communities.

As part of that, we've developed the role of Principal Advisor Māori into Pou Ārahi, to advise the organisation on privacy and community engagement from a Te Ao perspective.

We acknowledge that we have much to learn, but we're all committed to making the journey.



CASE STUDY TWO

Budget 2023 funding signals the importance of privacy rights

Budget 2023 provided OPC with additional funding of \$780,000 per annum. This will support the strengthening of our compliance and enforcement function, and the shift of the policy and advocacy function towards proactive work.

The funding came during a period of worldwide technological growth, where tools like biometrics and AI were creating challenges around how we ensure privacy regulation.

OPC has continued to record increases in privacy breach notifications and complaints around data security.

The changes we'll be making will help us provide agencies with greater certainty on their responsibilities. This will then be supported through guidance to agencies.





CASE STUDY THREE

Data insights a great privacy education tool

Education on privacy is a key function of OPC and helps agencies to better understand how the Privacy Act applies to them.

This programme of work includes our Insights Reports; short reports drawn from survey data on specific topics or themes. We published three Insights Reports during the 2022-2023 financial year.

Our rental sector report, which we researched and wrote in partnership with Consumer NZ, investigated how our new guidance on the data that landlords and property managers collected was being used.

The results showed that many property managers had found ways to circumvent the guidance on privacy, and that renters were likely to experience resistance from property managers should they try to assert their data-privacy rights.

A report on small businesses highlighted that, while business owners showed they understood personal information and privacy issues, they didn't always have relevant privacy policies and procedures in place.

It didn't matter whether a business was big or small, the privacy breach likelihood was about the same. With this information we were able to create materials for

businesses to use to help upgrade their privacy competency.

We produced a report on privacy in the digital age to remind people that they still had privacy rights, and could expect those rights to be respected online.

New Zealanders love the internet. We've seen this in our own statistics, with 60 percent of serious privacy breaches reported to OPC as happening online. Drawing content from OPC, InternetNZ, and New Zealand's cyber security agency CERT, we showed simple steps people could take to protect themselves. They included looking at how to keep children's privacy safe online, the secret costs of using social media, and how people could protect themselves from becoming victims of online fraud and scams.

The report was an education piece designed to demystify access to online privacy. People may not feel they have choices in what happens to their data, but the report helps people to take practical steps to limit the data that data agencies and others can access.

60%
serious breaches
are online



Objective 3 | Whāinga 3

We are trusted as a fair and responsive regulator

He meawhakawhirinaki mātou heikaiwhakarite tokeke, tika hoki

We aim to be trusted as a fair and responsive privacy regulator in Aotearoa New Zealand. Privacy is the foundation of trust, and we promote the importance of protecting it to organisations and the public.

Privacy is a right that all New Zealanders have, regardless of their age or circumstances.

A major component of our work as regulator is in education. A good example of that is when we worked with local councils affected by Cyclone Gabrielle to help ensure they knew how the Privacy Act related to that circumstance.

In March 2023, Cyclone Gabrielle had triggered the Civil Defence National Emergencies (Information Sharing) Code 2020, which allowed agencies to collect, use, and disclose personal information for purposes directly related to the government's and local government's response to the emergency.

The code of practice was created to make it easier for government agencies and local government teams to work together in a safe, planned way. But everything becomes more difficult in an urgent situation.

Proactive email communications from us ensured that councils and other agencies affected by the natural disaster had the information they needed to meet their privacy obligations. We engaged media with our messages and prioritised answering questions and providing guidance where appropriate, and in ways that were easy to understand and use in the crisis.

Trust is crucial to the work we do, and we build trust by making sure we're fair and responsive regardless of who we're doing business with.

In the compliance and enforcement area, this year we closed our first-ever Privacy Act compliance notice (issued to the Reserve Bank of New Zealand – Te Pūtea Matua in September 2021). Our second compliance notice, issued to New Zealand Police (December 2021), is still active.



CASE STUDY ONE

Working for clear and fair legislation

We've had a successful year in helping to guide legislative development as part of our role as a trusted privacy regulator.

This year, OPC:

- Supported the work of the Ministry of Justice in the development of the Privacy Amendment Bill.
- Supported the Ministry of Business, Innovation and Employment in its development of a Consumer Data Right for New Zealanders.
- Provided online guidance for whistleblowers on when it may be appropriate to raise serious concerns about privacy practices with OPC under the Protected Disclosures Act 2022.

The Privacy Amendment Bill focuses on the transparency principle in the Privacy Act; a useful principle when agencies are collecting personal information about individuals. It means they should be informing people on why they're collecting their personal information and who'll hold the information, and that those people can access their information and can request corrections of that information if it's not accurate.

We supported the proposed amendment to the Privacy Act to have a broader transparency requirement so that agencies needed to think about how to tell people they were collecting their information, regardless of its source.

This amendment is about keeping up with international best practice. It's important that our privacy framework keeps pace, particularly given the rising challenges of technology for citizens and consumers.



CASE STUDY TWO

Completing our joint report with the Independent Police Conduct Authority into Police photography

In March 2021, the Independent Police Conduct Authority and OPC launched a joint inquiry into complaints from the public about Police taking photographs of rangatahi who had not been suspected of committing crimes. During the inquiry, the Deputy Privacy Commissioner issued a compliance notice requiring the deletion of photographs and duplicate biometric prints of young people.

The joint report was released in September 2022 and found that a lack of awareness amongst the Police of their obligations under the Privacy Act had led to officers routinely taking, using, and retaining photographs when it was not lawful for them to do so. It was also discovered that thousands of photographs of members of the public had been kept on the mobile phones of individual officers or, if transferred to the Police computer system, not destroyed when there was no longer a legitimate need for them.

It was also discovered the Police had developed a practice of regularly taking duplicate sets of 'voluntary' fingerprints and photographs of youths who had ended up in Police custody for suspected offending, and retaining them for longer periods than permitted by the regime for compulsory prints and photographs under the Policing Act.

The Police accepted the findings of the joint report and released five progress reports on work towards meeting the requirements of the compliance notice issued in December 2021. The Police are working through their compliance notice with the OPC compliance and enforcement team and meet quarterly with us.

The Privacy Commissioner may issue compliance notices to organisations and businesses that are not meeting their obligations under the Privacy Act. It requires the organisations and businesses to do something, or to stop doing something, to comply. Once we issue a notice, we work alongside the business or organisation to make sure that the necessary system changes are being implemented.





CASE STUDY THREE

We continued our work on the current regulation of biometrics

This year our Policy team progressed its work on biometrics to the point where it was time to start a conversation with stakeholders about exploring a potential code for biometrics as an option for regulation. This engagement will be part of our next reporting period in 2023-2024. The aim that underlies this work is to provide people and agencies with guidance on their privacy rights and obligations when using biometrics and biometric technologies.

After running an initial consultation process, the team prioritised biometrics as a work focus. The Policy team redirected resources while biometric technologies were beginning to be introduced by New Zealand companies, after developing at a significant pace internationally.

While these technologies can be used safely and beneficially, particularly to provide secure and efficient verifications of people's identities, they can also pose significant privacy risks and have potential for harm.

In OPC's position paper on biometrics, we said organisations should take appropriate steps to identify and respond to the impacts on, and concerns from, the public. As a modern and responsive regulator, OPC stepped up efforts to make sure the regulatory framework was examined and investigated, and also focused on ensuring there was enough time for interested groups, including those developing approaches to Māori data sovereignty, to be brought into the conversation.





Objective 4 | Whāinga 4

We influence privacy practices and behaviour

Ka whakaawe mātou i ngā mahi me ngā whanonga matatapu

We work to ensure we're positively influencing organisations to develop their own workplace cultures founded on respecting personal information. Our ability to influence has been essential in the past year to ensuring privacy is a central consideration for government when it creates and implements policy and law.

More than ever, people and agencies are reporting privacy breaches. Our role is to run a fair complaints process, ensure regulation for agencies, and educate New Zealanders about privacy. How we do that sets the tone for privacy practices and behaviour.

It's very clear that New Zealanders care about their privacy and how agencies handle their information – especially when a privacy breach occurs. Research undertaken by Internet NZ in March 2023 showed the public had concerns about online crime, security of personal data, and threats to privacy. It showed that in the past 12 months that two-thirds of New Zealanders had chosen not to use at least one online service because of security and privacy concerns.

Awareness often brings a very good opportunity to influence change, and this year we've been vocal in speaking out on issues, especially in media, to influence privacy practices. We've told New Zealanders it's okay to ask why an agency wants their information. We've encouraged the use of two-factor authentication and the Commissioner has issued his expectations of agencies when using generative AI.

We regularly advise agencies that report they are the victims of malicious cyber-attacks to take steps to seek injunctions from the High Court to protect compromised data. Injunctions are an increasingly important tool for agencies, particularly health and education agencies, that experience serious privacy breaches.

We're increasingly seeing our key message that "privacy should be as important for an organisation as health and safety" repeated by media commentators and legal bodies. The Commissioner, Deputy Commissioner, and our Office privacy experts speak to diverse groups across the motu, including the New Zealand government through its Data, Digital and Security Summit, the Financial Services Federation, the Marketing Association, the International Association of Privacy Professionals, the New Zealand Law Society, and the New Zealand Bar Association.



CASE STUDY ONE

Injunctions a powerful tool in the privacy toolkit

When Mercury IT experienced a cyber-attack in late 2022, and obtained a court injunction to protect its information, we released a media advisory to highlight the injunction and to remind people not to access or share compromised data.

Protecting people in the middle of a fast-moving data breach must always be prioritised.

The High Court's permanent injunction in February 2023 to stop people storing, publishing, sharing, or accessing files obtained from the attack on Mercury IT systems was great evidence of that. The key message was that it's vital that

people respect the personal information of others. Treat the information as you would expect others to treat yours if it were disclosed to you.

An interim injunction had been issued soon after the breach in December 2022. At the time, Privacy Commissioner Michael Webster said, "You have to act fast. It might sound drastic, but reaching out to the courts can help prevent further harm by making it clear to everyone that no one should breach the confidences that apply to compromised data."

The injunction applies to everyone, from individuals to the news media and bloggers.

"You have to act fast. It might sound drastic, but reaching out to the courts can help prevent further harm by making it clear to everyone that no one should breach the confidences that apply to compromised data."



CASE STUDY TWO

Privacy Week delivers to more than 4,700 people

Passionate privacy professionals have always valued Privacy Week, but this year we aimed it at newcomers too.

Privacy Week, which is OPC's annual week of privacy-focused events, was dedicated to digital issues given the rise in cyber-attacks and an increase in fast-evolving technologies, and the potential impacts on the public. The more that people understand privacy and their rights, the stronger the community engagement can be.

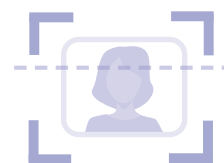
To help our audience self-select what was best for them, we asked presenters to rank their webinars as beginner, intermediate, or experienced.

Digital knowledge had increased since the COVID-19 lockdown, and we knew people would be confident with Zoom, so the whole event was held online, with 20 webinars hosted by a range of high-calibre academics and professional speakers. Having a digital event meant it didn't matter where in the world people were. In one talk we had a speaker from Poland and another from Barbados presenting together to an audience in New Zealand.

Topics included biometrics, Māori data sovereignty, rural farming tools, the ethics of AI, and online dating and privacy. It was important for OPC that we had a programme where people of all backgrounds could access privacy-related topics that were of interest to them.

Our most popular talk had over 700 people attend. In 2022 the talks held online had an average sign-up of 180 people. In 2023 that number grew to 443.

The numbers tell the story. People were eager to learn about privacy and wanted that information delivered in a convenient way.





CASE STUDY THREE

You can tell the story without telling the whole story

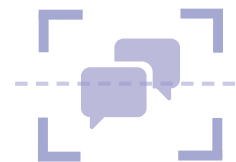
The Health and Disability Commissioner referred a medical practice to OPC in 2022. The incident had begun with a misunderstanding of a medical procedure.

After the procedure was completed, the patient notified the practitioner that they were intending to lodge a complaint with the governing medical board.

Once the patient had left the clinic, the medical practitioner contacted a retired member of their medical field. This retiree happened to be a neighbour of the affected patient. In this conversation, the identity of the patient was revealed, and once the conversation concluded, the retiree contacted the patient to discuss the complaint. The patient felt their privacy had been breached and asked the medical practice to apologise. They received no reply.

After an investigation was conducted, the medical practice issued an apology to the patient and provided further training for staff using tools on OPC's website.

Small and large businesses can use this as an example of how even well-intentioned actions can breach people's privacy if the proper precautions are not taken. There was no problem with the medical practitioner contacting a professional within their field for advice, but revealing the name and any identifying details of the patient was not necessary in that discussion.



Office and functions | Te Tari me āna mahi



Independence and competing interests | Te noho motuhake me te taupatupatu o ngā hiahia

The Privacy Commissioner has wide ranging functions. The Commissioner must have regard to the information privacy principles in the Privacy Act and the protection of important human rights and social interests that compete with privacy.

Competing social interests include the desirability of a free flow of information and the right of government and business to achieve their objectives in an efficient way. The Commissioner must take account of New Zealand's international obligations and consider any general international guidelines that are relevant to improved protection of individual privacy.

The Privacy Commissioner is independent of the Executive. This means the Commissioner is free from influence by the Executive when investigating complaints, including those against Ministers or their departments. Independence is also important when examining the privacy implications of proposed new laws and information matching programmes.

Reporting | Te tuku pūrongo

The Privacy Commissioner reports to Parliament through the Minister of Justice and is accountable as an independent Crown entity under the Crown Entities Act 2004.

Staff | Kaimahi

We employ staff in our Auckland and Wellington offices. During the year to 30 June 2023, the senior leadership team was made up as follows:

-  **The Deputy Commissioner, Policy and Operations:** responsible for 3 teams – Investigations and Dispute Resolution, Policy, and Compliance and Enforcement.
-  **The Assistant Commissioner, Strategy, Policy and Engagement:** responsible for the Strategy and Insights team and Communications and Engagement team.
-  **The General Manager:** responsible for administrative and managerial services. We employ administrative support staff in both offices.
-  **The General Counsel:** legal counsel to the Privacy Commissioner, manages litigation, and gives advice around investigations and law reforms.

Statutory remuneration disclosures | Whakapuakitanga ā-Ture i ngā Taiutu

1 July 2022 – 30 June 2023

The Office of the Privacy Commissioner is a Crown Entity and is required to disclose certain remuneration information in its annual reports. The disclosures required are set out in Section 152 of the Crown Entities Act 2004 (CEA).

Employees' Remuneration

The number of employees receiving total remuneration of \$100,000 or more per annum is disclosed below in \$10,000 bands. This table does not include the Commissioner as he is disclosed separately below.

Total remuneration and benefits	Number of employees	
	Actual 2023	Actual 2022
\$100,000 – \$109,999	4	3
\$110,000 – \$119,999	1	1
\$120,000 – \$129,999	2	1
\$130,000 – \$139,999	3	1
\$140,000 – \$149,999	-	1
\$150,000 – \$159,999	-	2
\$160,000 – \$169,999	1	1
\$170,000 – \$179,999	1	-
\$180,000 – \$189,999	1	2
\$200,000 – \$209,999	1	-
\$240,000 – \$249,999	-	2
\$320,000 – \$329,999	-	1
\$340,000 – \$349,999	1	-

Commissioners' total remuneration

In accordance with the disclosure requirements of section 152(1)(a) of the CEA, the total remuneration, as set independently by the Remuneration Authority, includes all benefits paid during the period 1 July 2022 to 30 June 2023.

Name	Position	Amount 2023	Amount 2022
Michael Webster	Privacy Commissioner (from July 2022)	396,704	-
John Edwards	Privacy Commissioner (to 31 December 2021)	-	241,546
Liz MacPherson	Acting Privacy Commissioner*	-	211,769

*In the 2022 year, the Acting Privacy Commissioner role commenced from 10 December until the new Commissioner was appointed in July 2022.

Cessation payment

During the 2023 year, there were no payments made in relation to cessation (2022: \$nil).

Indemnity and Insurance disclosures

The Privacy Commissioner's insurance policy covers public liability of \$10million and professional indemnity of \$1million.

EEO profile | Pūkete EEO

The Office of the Privacy Commissioner promotes Equal Employment Opportunities (EEO) to ensure our people capability practices are in line with our obligations as a good employer.

We have an EEO policy integrated into the human resource programmes that are outlined in our Statement of Intent 2020-2024. The policy encourages active staff participation in all EEO matters. We likewise have policies on employee development, harassment prevention, and health and safety, and employee-led groups for Health, Safety and Wellbeing, and diversity and inclusion.

In November 2022 we published our Kia Toipoto Action Plan on our website¹. This sets out the Office's response to the Public Service Pay Gap Action Plan aimed at closing the gender, Māori, Pacific, and ethnic pay gaps, and creating fairer workplaces for all. The Plan identifies 6 areas of focus and reports on the Office's progress against each and identifies areas for continuous improvement.

The 6 areas under the Kai Toipoto Action Plan are as follows: –

- ✓ **Te Pono – Transparency:** Ensuring easy access to HR and remuneration policies.
- ✓ **Ngā Hua Tōkeko mō te Utu – Equitable pay outcomes:** Ensuring that starting salaries and salaries for the same or similar role are equitable.
- ✓ **Te whai kanohi i nga taumata katoa – Leadership and representation:** Strengthening gender and ethnic representation.
- ✓ **Te Whakawhanaketanga i te Aramahi – Effective career and leadership development:** Ensuring opportunities are transparent and inclusive and promote participation.
- ✓ **Te whakakore i te katoa onga momo whakatoihara haukume anō – Eliminating all forms of bias and discrimination:** Building and affinity and understanding of Te Ao Māori and other cultural values.
- ✓ **Te Taunoa o te Mahi Pīngore – Flexible-work-by-default:** Offering flexible work by default.

1. This can be found here <https://www.privacy.org.nz/about-us/transparency-and-accountability>

Whilst we do not currently, for privacy reasons, ask staff to self-identify their ethnicity, we do usually have some mix of ethnicities across the Office.

We also do not collect information on employees' age, gender or disabilities. Where a disability is brought to our attention, we take steps to ensure that the employee has the necessary support to undertake their duties.

Our recruitment policies, including advertisement, comply with the good employer expectations of Diversity Works New Zealand, of which we are a member.

We have formal policies regarding bullying, harassment, and the provision of a safe and healthy workplace. Staff have ready access to external support through an employee assistance programme.



November 2022

We published our Kia Toipoto Action Plan on our website. This sets out the Office's response to the Public Service Pay Gap Action Plan aimed at closing the gender, Māori, Pacific, and ethnic pay gaps, and creating fairer workplaces for all.



Workplace FTE profile

as at 30 June 2023

Role	Number of staff			Total
	Full-time	Part-time	Fixed Term	
Commissioner	1			1
Deputy Commissioner	1			1
Senior managers	3			3
Team and unit managers	4	2		6
Investigations and Dispute Resolution	7	2		9
Administrative support	6	2		8
Policy	6*	1	2	9
Compliance and Enforcement	6			6
Strategy, Insights and Communications	4	2		6
Legal	1	1		2
Total	39	10	2	51

*One FT role on secondment as at 30 June 2023.

Finance and performance report | Pūrongo whakahaere pūtea me ngā tutukitanga



Statement of responsibility | Tauākī noho haepapa

Under the Crown Entities Act 2004, the Privacy Commissioner is responsible for the preparation of the financial statements and statement of performance, and for the judgements made in them.

We are responsible for any end-of-year performance information provided by the Privacy Commissioner under section 19A of the Public Finance Act 1989.

The Privacy Commissioner has the responsibility for establishing and maintaining a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial and performance reporting.

In the opinion of the Privacy Commissioner, these financial statements and statement of performance fairly reflect the financial position and operations of the Privacy Commissioner for the year ended 30 June 2023.



M Webster
Privacy Commissioner
31 October 2023



E Boddy
General Manager
31 October 2023

Statement of performance | Tauākī tutukitanga





The Justice Sector has an aspirational outcome that all New Zealanders should expect to live in a safe and just society. We support this aspiration as a Justice Sector Crown entity.

While the Office of the Privacy Commissioner is an independent Crown entity and strongly maintains such independence, our Statement of Intent and Statement of Performance Expectations set out a work programme that complements this aspiration and government priorities as a whole.

Our Statement of Intent 2020-2024 identifies four high level objectives to support our mission to be an “effective modern privacy regulator”. The “Strategic objectives progress” section of this Annual Report provides specific evidence on how the Office has performed against each of these objectives during the year.

In addition to the high-level objectives, the Office also identified two strategic priorities for the 2022/23 year – Rental Sector and Embedding Te Ao Māori perspectives into our work. A summary of the key work undertaken within each of these areas is also highlighted in the section noted above.

The Statement of Performance Expectations for the year to June 2023 identified five output areas (Primary Activities) to support these four objectives and priorities. These are consistent with the previous year and we report our progress against these Primary Activities in this section with linkage through to the objectives, where appropriate, using the following symbols:-

-  **Objective 1** – Privacy protection is effective and easy to achieve
-  **Objective 2** – Costs of privacy compliance are minimised
-  **Objective 3** – OPC is trusted as a fair and responsive regulator
-  **Objective 4** – OPC influences privacy practices and behaviours

Impact of Natural Disasters and COVID-19 on performance

New Zealand has been impacted by the COVID-19 pandemic over the past few years and more recently by the severe weather events in early 2023. Whilst the overall risks and uncertainties associated with COVID-19 continue to reduce, and the weather events did not directly impact on the Auckland and Wellington Offices, the Office does continue to monitor the impacts as part of its wider Risk Management Plan.

During the year, the Office undertook an IT upgrade to provide Laptops to all staff. This is part of the Office wide Business Continuity plan and has enabled staff to continue to work from home and to ensure that service delivery continues.

Reliable data and information has remained available throughout the year in order to report against all measures, and performance against most measures has been achieved. This is consistent with the prior year.

The risks will continue to be monitored by the Senior Leadership Team and also through the internal Legislative Compliance Working Group and Health, Safety and Wellbeing Committee.

PBE FRS 48

service performance reporting |

PBE FRS 48 Pūrongo Tutukitanga Ratonga

PBE FRS48 is effective for the year ending 30 June 2023 and has replaced the previous service performance reporting requirements of PBE IPSAS 1 Presentation of Financial Statements.

As noted above, the Statement of Intent covering the period 1 July 2020 to 30 June 2024 and the Statement of Performance Expectations for the year to 30 June 2023² each set out the longer-term strategy of the Office as well as the specific priorities set for the year to 30 June 2023. The two priorities identified for the 2023 year, were a continuation of areas identified in the 2022 year following a detailed analysis of themes from business intelligence sources as well as internal office discussions. The Office has however remained flexible to working on new priority areas, for example Biometrics and AI, as reported earlier.

How the measures were selected

The suite of Performance Measures for the 2023 year remained unchanged from the 2022 year, except for the removal of one measure in the Communication and Education Primary Activity area due to it being outside of the Office's control. The decision to retain the current suite of measures was made following consultation with both the Senior Leadership Team and the Operational Managers. As a detailed review of the KPIs had taken place in 2021, resulting in several changes, and with a new Statement of Intent being due from 1 July 2023, retention of the current suite was deemed appropriate.

The final proposed suite of measures is subject to a thorough review process, both internally and through the Estimates of Appropriation process with the Ministry of Justice to ensure consistency with Estimates set out in the Vote Justice document³. The Office considers feedback that it receives and makes changes it thinks are necessary or would improve overall reporting.

Judgements and measurement

A certain amount of judgement is required to be made when setting the targets against the measures. This judgement considers both previous performance as well as future expectations. No changes were made to the targets in the year to 30 June 2023.

As part of the annual review of measures, the Office also considers whether systems for capturing and recording the data are in place. Most of the data required for reporting is captured within the Office's document management system (see the Statement of Performance Expectations which sets out which measures rely on this data) and analysis is undertaken throughout the year, and at year-end, to ensure that the information is fit for purpose. No changes were required to be made to any internal systems as part of the reporting in the year to 30 June 2023.

Performance against three of the measures is based on an external assessment. Where this is the case, further information has been provided in the reporting that follows.

2. These documents can both be accessed on the Office's website.

3. See <https://www.treasury.govt.nz/sites/default/files/2022-06/est22-v6-just.pdf>

Statement specifying comprehensive income | Tāuāki tautohu whiwhinga whānui

The Privacy Commissioner agreed the following financial targets with the Minister at the beginning of the year:

Specified comprehensive income	Target \$000	Achievement \$000
Operating grant	7,392	7,392
Other revenue	163	219
Total revenue	7,555	7,611

The appropriation received by the Privacy Commissioner equals the government's actual expenses incurred in relation to the appropriations, which is a required disclosure from the Public Finance Act.

The operating grant is received as part of the Non-Departmental Output Expenses – Services from the Privacy Commissioner within Vote Justice. This appropriation is limited to the provision of services concerning

privacy issues relating to the collection and disclosure of personal information and the privacy of individuals.

The amount received by the Privacy Commissioner equates to 1.8% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2022/23. The total expenses in the year are \$7,460k as set out in the cost of service statement on the following pages.

Cost of service statement | Tauākī utu ratonga

for the year ended 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

As set out in the 2022/23 Statement of Performance Expectations, the Privacy Commissioner committed to provide five primary activities. The split of funds across these five primary activities is set out below:

	Actual 2023 \$000	Budget 2023 \$000	Actual 2022 \$000
PRIMARY ACTIVITY 1: COMMUNICATION AND EDUCATION			
Resources employed			
Revenue	1,048	1,042	1,020
Expenditure	1,059	1,091	994
Net Surplus/(Deficit)	(11)	(49)	26
PRIMARY ACTIVITY 2: ADVICE AND ADVOCACY			
Resources employed			
Revenue	1,508	1,494	1,561
Expenditure	1,462	1,462	1,334
Net Surplus/(Deficit)	46	32	227
PRIMARY ACTIVITY 3: COMPLIANCE AND ENFORCEMENT			
Resources employed			
Revenue	1,731	1,720	1,801
Expenditure	1,679	1,688	1,549
Net Surplus/(Deficit)	52	32	252
PRIMARY ACTIVITY 4: INVESTIGATION AND DISPUTE RESOLUTION			
Resources employed			
Revenue	1,865	1,846	1,957
Expenditure	1,821	1,829	1,694
Net Surplus/(Deficit)	44	17	263

	Actual 2023 \$000	Budget 2023 \$000	Actual 2022 \$000
PRIMARY ACTIVITY 5: STRATEGY AND INSIGHTS			
Resources employed			
Revenue	1,459	1,453	1,458
Expenditure	1,439	1,479	1,361
Net Surplus/(Deficit)	20	(26)	97
TOTALS			
Resources Employed			
Revenue	7,611	7,555	7,797
Expenditure	7,460	7,549	6,932
Net Surplus/(Deficit)	151	6	865

The following tables sets out the assessment of our performance against the targets set out in the Statement of Performance Expectations. They also reflect the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation. The following grading system has been used which is consistent with prior years:

Criteria	Rating
On target or better	Achieved
<5% away from target	Substantially achieved
>5% away from target	Not achieved



Primary activity 1 | Mahi matua 1

Strategy and insights | Rautaki me ngā

Activity areas of focus

Understanding trends and technological developments that will be relevant in the future. Using evidence based on all inputs, including complaints, media, breach reporting, enquiries, international regulators or website analytics, to prioritise work and make decisions. Monitor success of strategies and initiatives. Advising the Commissioner on the best way to achieve the Office's mission as well as associated risks.

Output Measures

Measure	Estimate	Achieved 2022/23	Achieved 2021/22
Number of cross office priorities focussed on globally identified privacy trends or systematic issues. 	4	Achieved – 4 During the year, the Office has been focussed on the Rental Sector, Biometrics, the IPCA joint inquiry and embedding Te Ao Māori perspectives.	Achieved – 4 During the year, the Office was focussed on the following priority areas – Rental Sector, Biometrics, Embedding Te Ao Māori perspectives and the IPCA joint inquiry.
Number of published “insights” reports on trends that the office is seeing. ⁴ 	3	Achieved – 3 The Office has published Insights Reports covering the Rental Sector (September 2022), Small Businesses (May 2023) and Protecting your Privacy in the digital age (June 2023).	Not achieved – 2 In December 2021, the Office published an Insights Report on Privacy Breach Reporting and a further report was published in May 2022 covering awareness, knowledge and levels of concern regarding privacy amongst the general public.

4. This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.


Primary activity 2 | Mahi matua 2

Communications and education | Whakapāpātanga, mātauranga hoki

Activity areas of focus

Informing people about their privacy rights. Promoting privacy understanding and competence, using media, opinion writing, events and conferences, stakeholder engagement. Producing material and resources to inform, guide and educate. Reduce the need for enforcement and dispute resolution through education.

Output Measures

Measure	Estimate	Achieved 2022/23	Achieved 2021/22
Education module completions as a percentage of education module registrations in the year. 	75%	Achieved – 79%	Achieved – 79%
Percentage of media enquiries that are responded to within 2 working days. 	100%	Substantially Achieved – 98% Of the 202 media enquiries received, 198 were responded to within 2 working days.	Achieved – 100% All of the 184 media enquiries were responded to within 2 working days.
Respond to all enquiries within 2 working days. ⁵ 	95%	Achieved – 95%	Substantially achieved – 94%

5. Please refer to footnote 4.




Primary activity 3 | Mahi matua 3

Compliance and enforcement | Te tautukunga me te whakauruhi

Activity areas of focus

Identifying and assessing systematic issues, using the right tools to get the best privacy outcomes for New Zealanders, including enforcing the Codes, managing privacy breach responses, prosecution, monitoring of compliance, enforcement of policy work to ensure compliance.

Output Measures

Measure	Estimate	Achieved 2022/23	Achieved 2021/22
<p>The percentage of data breach notifications received through NotifyUs that are triaged within 1 working day.⁶</p> 	95%	Achieved – 96%	Achieved – 95%
<p>The percentage of externally reviewed compliance notices and Access Directions issued that meet quality review standards.⁷</p> 	100%	<p>Achieved – 100%</p> <p>The review was undertaken by an external consulting firm and the result is based on a review of the one Compliance Notice issued in the year (no Access Directions were issued).⁸ Criteria are set out below.</p>	<p>Not measured</p> <p>An external review was not undertaken this year due to the low number of notices and access directions issued.</p>
<p>The percentage of information matching files reviewed within the mandatory 5-year period as required under S184 of the Privacy Act.</p> 	100%	<p>Achieved</p> <p>7 Information matching provisions were required to be reviewed in the year. All were reviewed and reported on as required.</p>	<p>Achieved</p> <p>All reviews are up to date although no information matching provisions were due a 5-year review in the 12 months to 30 June 2022.</p>

6. Please refer to footnote 4.

7. Please refer to footnote 4.

8. When assessing the quality, the reviewer explored the factors that need to be considered when issuing a notice and whether this provided a sound basis to make a decision, whether the process for issuing the notice was properly followed and whether specific content required by the Privacy Act 2020 was fully and accurately included. A score of 3.5 out of 5 was given, and in-line with the external reviews of both policy and complaint files, the KPI is “achieved”.

Primary activity 4 | Mahi matua 4




Advice and advocacy |

Te tohutohu me te taunaki

Activity areas of focus

Research and analysis supports advice on privacy issues that is context aware, evidence based and clear and informed. Advice reflects diverse perspectives and recognises risks and competing interests. Effective interventions include the development of privacy codes and advice to government on changes to other legislation. Advocate for privacy positive outcomes, including privacy by design.

Output Measures

Measure	Estimate	Achieved 2022/23	Achieved 2021/22
<p>The percentage of externally reviewed policy and information sharing are rated as 3.5 out of 5 or better for quality.⁹</p> 	85%	<p>Not achieved – 80%</p> <p>The review was undertaken by an external consulting firm and the result is based on a review of a sample of 10 files (7%) in the year randomly selected by the reviewer. Criteria are set out below.¹⁰</p>	<p>Achieved – 95%</p>
<p>The Commissioner actively contributes on advice, guidelines and directions by international institutions and guiding bodies, relating to the advancement of privacy rights, where it is in New Zealand's interest to do so.</p>  	Achieved	<p>Achieved</p> <p>The Office of the Privacy Commissioner has continued to support the development of international advice, guidelines, and directions, over the past year.</p> <p>We have been closely engaged in supporting the Ministry of Justice and Ministry of Foreign Affairs in discussions with the European Union on New Zealand's adequacy status. We have also attended multiple iterations of the Asia Pacific Privacy Authorities (APPA) forum, as well as the Global Privacy Assembly in October 2022, where we engaged in a range of discussions on pressing privacy matters and supported resolutions.</p>	<p>Achieved</p> <p>The Office of the Privacy Commissioner has continued to support the development of international advice, guidelines, and directions, over the past year.</p> <p>We have been closely engaged in supporting the Ministry of Justice and Ministry of Foreign Affairs in discussions with the European Union on New Zealand's adequacy status. We have also attended multiple iterations of the Asia Pacific Privacy Authorities (APPA) forum, as well as the Global Privacy Assembly in October 2021, where we engaged in a range of discussions on pressing privacy matters and supported resolutions.</p>

9. Please refer to footnote 4.

10. The files were reviewed against the quality standards established by the Policy Project and required for all government agencies with policy appropriations from July 2019. The assessment focussed on context, analysis, advice and actions outlined in each file reviewed. It also included an assessment of the incorporation of Treaty and Te Ao Māori analysis as necessary. Each file was assigned a score from 1 to 5 with 1 being unacceptable and 5 being excellent. An overall average score was calculated across all files reviewed and this was based on the judgement of the reviewer.




Primary activity 5 | Mahi matua 5

Investigations and dispute resolution | Ngā whakatewhatewha, whakatau tautohe hoki

Activity areas of focus

Working with parties to achieve a fair outcome using dispute resolution techniques in the first instance. Investigating individual complaints where dispute resolution is inappropriate or unsuccessful. Declining to investigate cases where investigations are unnecessary or inappropriate. Referring serious cases to the Director of Human Rights Proceedings and issuing compliance notices and access directions.

Output Measures

Measure	Estimate	Achieved 2022/23	Achieved 2021/22
<p>The percentage of notified complaints files closed by settlement between the parties.¹¹</p> 	40%	Achieved – 69%	Achieved – 63% The office has continued to focus on reaching settlement in the year.
<p>The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.¹²</p> 	90%	Achieved – 100% The review was undertaken by a Barrister external to the Office and the result is based on a review of a sample of 15 files closed in the year randomly selected by the reviewer. Specific criteria are set out below. ¹³	Achieved – 100%
<p>The percentage of complaint files closed during the year that were less than 6 months old at closure.¹⁴</p> 	85%	Not achieved – 49% In addition to the complaint files closed in the year, the Office has also closed 534 “Fast Resolve” complaints. Including these would increase the result to 82% closed within 6 months.	Not achieved – 67% The office has had fewer, more complex complaints to deal with. Due to the nature of these complaints, the time taken to resolve them has taken longer but the rate of settlement (as seen above) has remained high.

11. Please refer to footnote 4.

12. Please refer to footnote 4.

13. Files were assessed for quality of legal analysis, correctness of legal conclusions, processes accord with the law, processes accord with best investigative/resolution/determinative practice and staff are following OPC policies in handling complaints. Each area was assigned a score of between 1-5 with 1 being not acceptable and 5 being outstanding. An average for each file was then calculated. The scoring was based on the judgement of the Reviewer, who was the same as in 2022.

14. Please refer to footnote 4.

Statement of accounting policies | Tauākī kaupapa-here kaute

for the year ended 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

Reporting entity

These are the financial statements of the Privacy Commissioner, a Crown entity in terms of the Public Finance Act 1989 and the Crown Entities Act 2004. As such the Privacy Commissioner's ultimate parent is the New Zealand Crown.

These financial statements have been prepared in accordance with the requirements of the Crown Entities Act 2004.

The Privacy Commissioner's primary objective is to provide public services to the New Zealand public, as opposed to that of making a financial return. Accordingly, the Privacy Commissioner has designated itself as a public benefit entity for financial reporting purposes.

The financial statements for the Privacy Commissioner are for the year ended 30 June 2023 and were approved by the Commissioner on 31 October 2023. The financial statements cannot be altered after they have been authorised for issue.

Basis of preparation

The financial statements have been prepared on a going concern basis, and the accounting policies have been applied consistently throughout the period.

Statement of compliance

The financial statements of the Privacy Commissioner have been prepared in accordance with the requirements of the Crown Entities Act 2004, which includes the requirement to comply with New Zealand generally accepted accounting practice ("NZ GAAP").

The financial statements have been prepared in accordance with Tier 2 PBE accounting standards. The Tier 2 criteria have been met as expenditure is less than \$30m and the Privacy Commissioner is not publicly accountable (as defined in XRB A1 Accounting Standards Framework).

These financial statements comply with PBE accounting standards.

Measurement base

The financial statements have been prepared on a historical cost basis.

Functional and presentation currency

The financial statements are presented in New Zealand dollars and all values are rounded to the nearest thousand dollars (\$000). The functional currency of the Privacy Commissioner is New Zealand dollars.

Summary of significant accounting policies

Significant accounting policies are included in the notes to which they relate.

Significant accounting policies that do not relate to specific notes are outlined below.

Budget figures

The budget figures are derived from the Statement of Performance Expectations as approved by the Privacy Commissioner at the beginning of the financial year.

The budget figures have been prepared in accordance with generally accepted accounting practice and are consistent with the accounting policies adopted by the Privacy Commissioner for the preparation of the financial statements.

Cost allocation

The Privacy Commissioner has determined the costs of outputs using a cost allocation system as outlined below.

Direct costs are those costs directly attributed to an output. These costs are therefore charged directly to the outputs.

Indirect costs are those costs that cannot be identified in an economically feasible manner with a specific output. Personnel costs are charged based on % of time spent in relation to each output area. Other indirect costs are allocated based on the proportion of staff costs for each output area.

There have been no substantial changes to the cost allocation methodology since the date of the last audited financial statements.

Goods and Services Tax (GST)

All items in the financial statements presented are exclusive of GST, with the exception of accounts receivable and accounts payable, which are presented on a GST inclusive basis. Where GST is irrecoverable as an input tax, then it is recognised as part of the related asset or expense.

The net amount of GST recoverable from, or payable to, the Inland Revenue Department (IRD) is included as part of receivables or payables in the statement of financial position.

The net GST paid to, or received from IRD – including the GST relating to investing and financing activities – is classified as an operating cash flow in the statement of cash flows.

Commitments and contingencies are disclosed exclusive of GST.

Income tax

The Privacy Commissioner is a public authority for tax purposes and therefore exempt from income tax. Accordingly, no provision has been made for income tax.

Financial instruments

The Privacy Commissioner is party to financial instruments as part of its normal operations. These financial instruments include bank accounts, short-term deposits, debtors, and creditors. All financial instruments are recognised in the statement of financial position and all revenues and expenses in relation to financial instruments are recognised in the statement of comprehensive revenue and expenses.

Critical accounting estimates and assumptions

In preparing these financial statements the Privacy Commissioner has made estimates and assumptions concerning the future. These estimates and assumptions may differ from the subsequent actual results. Estimates and assumptions are continually evaluated and are based on historical experience and other factors, including expectations of future events that are believed to be reasonable under the circumstances.

The estimates and assumptions that have a significant risk of causing a material adjustment to the carrying amounts of assets and liabilities within the next financial year are:

- useful lives and residual values of property, plant and equipment – refer to Note 8
- useful lives of software assets – refer to Note 9.

Critical judgements in applying the Privacy Commissioner's accounting policies

Management has exercised the following critical judgements in applying the Privacy Commissioner's accounting policies for the period ended 30 June 2023:

- Lease classification – Refer Note 4
- Non-Government grants – Refer Note 2
- Grant expenditure – Refer Note 4

Statement of comprehensive revenue and expenses | Tauākī whiwhinga, whakapaunga whānui

for the year ended 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

	Note	Actual 2023 \$000	Budget 2023 \$000	Actual 2022 \$000
Revenue				
Crown revenue	2	7,392	7,392	7,392
Other revenue	2	219	163	405
Total income		7,611	7,555	7,797
Expenditure				
Promotion	4	51	130	97
Audit fees		64	35	34
Depreciation and amortisation	4,8,9	273	312	294
Rental expense		432	436	427
Operating expenses		1,204	1,134	974
Contract services		76	74	90
Staff expenses	3	5,360	5,428	5,016
Total expenditure		7,460	7,549	6,932
Surplus		151	6	865
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		151	6	865

Explanation of major variances are provided in Note 1.

The accompanying notes and accounting policies form part of those financial statements.

Statement of changes in equity | Tauākī rerekētanga o te whai tūtanga

for the year ended 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

	Note	Actual 2023 \$000	Budget 2023 \$000	Actual 2022 \$000
Total equity at the start of the year		2,446	2,310	1,581
Total comprehensive revenue and expenses for the year		151	6	865
Total equity at the end of the year	5	2,597	2,316	2,446

Explanations of major variances are provided in Note 1.

The accompanying notes and accounting policies form part of these financial statements.

Statement of financial position | Tauākī Tūnga Pūtea

as at 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

	Note	Actual 2023 \$000	Budget 2023 \$000	Actual 2022 \$000
Public equity				
General funds	5	2,597	2,316	2,446
Total public equity		2,597	2,316	2,446
Current assets				
Cash and cash equivalents	6	2,389	2,048	2,008
Receivables	7	82	29	57
Prepayments	7	144	100	158
Total current assets		2,615	2,177	2,223
Non-current assets				
Property, plant and equipment	8	305	217	380
Intangible assets	9	91	343	255
Capital work in progress	8,9	–	–	–
Total non-current assets		396	560	635
Total assets		3,011	2,737	2,858
Current liabilities				
Payables	10	158	150	147
Employee entitlements	12	247	260	249
Total current liabilities		405	410	396
Non-current liabilities				
Lease incentive	11	9	11	16
Total non-current liabilities		9	11	16
Total liabilities		414	421	412
Net assets		2,597	2,316	2,446

The accompanying notes and accounting policies form part of these financial statements.

Statement of cash flows | Tauākī kaupapa-here kaute

for the year ended 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

	Actual 2023 \$000	Budget 2023 \$000	Actual 2022 \$000
CASH FLOWS FROM OPERATING ACTIVITIES			
Cash was provided from:			
Receipts from the Crown	7,392	7,392	7,392
Receipts from other revenue	129	166	395
Interest received	70	2	6
Cash was applied to:			
Payment to suppliers	1,810	1,794	1,685
Payments to employees	5,361	5,415	5,166
Net Goods and Services Tax	5	(46)	(27)
Net cash flows from operating activities	415	397	969
CASH FLOWS FROM INVESTING ACTIVITIES			
Cash was applied to:			
Purchase of property, plant and equipment and intangibles	34	150	233
Cash was provided from:			
Sale of property, plant, and equipment and intangibles	–		–
Net cash flows from investing activities	(34)	(150)	(233)
Net increase/(decrease) in cash held	381	247	736
Plus opening cash	2,008	1,801	1,272
Closing cash balance	2,389	2,048	2,008
Cash and bank	2,389	2,048	2,008

The GST (net) component of operating activities reflects the net GST paid and received with the Inland Revenue Department. The GST (net) component has been presented on a net basis, as the

gross amounts do not provide meaningful information for financial statement purposes.

The accompanying notes and accounting policies form part of these financial statements.

Notes to the financial statements | He pitopito kōrero mō ngā tauākī kaute

for the year ended 30 June 2023 |
mō te tau i eke i te 30 o Pipiri 2023

Note 1: Explanation of major variances against budget

Explanations for significant variations from the Privacy Commissioner's budgeted figures in the Statement of Performance Expectations are as follows:

Statement of comprehensive revenue and expenses

The year-end reported surplus is higher than the budgeted surplus by \$145k. This is primarily due to the following:

Staff expenses (down on budget by \$68k)

Staff departures and a number of vacancies have resulted in the salary costs being lower than budgeted.

Promotion costs (down on budget by \$79k)

The costs associated with the annual Privacy Awareness Week/Forum and Education services were less than predicted. As in the prior year, Privacy Week including running a series of online talks and conversations rather than running any large in-person events. In addition, the budget had included some costs towards website upgrades but scoping and timing for this work is still to be undertaken.

Other operating expenses (up on budget by \$70k)

The 2 areas main areas different to budget were Computer and Network costs (over budget by \$130k), and Litigation (under budget by \$97k). The Office has continued to experience an increase in monthly license costs and Cloud related costs throughout the year, in addition to some one-off costs associated with computer and system upgrades.

Note 2: Revenue

Accounting policy

The specific accounting policies for significant revenue items are explained below:

Revenue from the Crown

The Privacy Commissioner is primarily funded through revenue received from the Crown, which is restricted in its use for the purpose of the Privacy Commissioner meeting his/her objectives as specified in the Statement of Intent and Statement of Performance Expectations.

The Privacy Commissioner considers there are no conditions attached to the funding and it is recognised as revenue at the point of entitlement.

The fair value of revenue from the Crown has been determined to be equivalent to the amounts due in the funding arrangements.

Other grants

Non-government grants are recognised as revenue when they become receivable unless there is an obligation in substance to return the funds if conditions of the grant are not met. If there is such an obligation the grants are initially recorded as grants received in advance and recognised as revenue when conditions of the grant are satisfied.

Interest

Interest revenue is recognised by accruing on a time proportion basis.

Provision of services

Revenue derived through the provision of services to third parties is treated as exchange revenue and recognised in proportion to the stage of completion at the balance sheet date.

Critical judgements in applying accounting policies

Non-government grants

The Privacy Commissioner must exercise judgement when recognising grant income to determine if conditions of the grant contract have been satisfied. This judgement will be based on the facts and circumstances that are evident for each grant contract.

Crown revenue

The Privacy Commissioner has been provided with funding from the Crown for specific purposes of the Privacy Commissioner as set out in its founding legislation and the scope of the relevant government appropriations. Apart from these general restrictions, there are no unfulfilled conditions or contingencies attached to government funding (2022: \$nil).

Other revenue breakdown

	Actual 2023 \$000	Actual 2022 \$000
Other grants received	116	316
Other revenue	33	83
Interest revenue	70	6
Total other revenue	219	405

Note 3: Staff expenses

Accounting policy

Superannuation schemes

Defined contribution schemes

Obligations for contributors to Kiwi Saver and the Government Superannuation Fund are accounted for as defined contribution superannuation schemes and are recognised as an expense in the statement of comprehensive revenue and expenses as incurred.

Breakdown of staff costs and further information

	Actual 2023 \$000	Actual 2022 \$000
Salaries and wages	5,143	4,982
Employer contributions to defined contribution plans	180	136
Other staff expenses	39	49
Increase/(decrease) in employee entitlements	(2)	(151)
Total staff expenses	5,360	5,016

Note 4: Other expenses

Accounting policy

Operating leases

Operating lease expenses are recognised on a straight-line basis over the term of the lease.

Grant expenditure

Discretionary grants are those grants where the Office of the Privacy Commissioner has no obligation to award the grant on receipt of the grant application. Discretionary grants with substantive conditions are expensed when the grant conditions have been satisfied.

Critical judgements in applying accounting policies

Grant expenditure

During the 2020 financial year, the Privacy Commissioner approved 4 discretionary grants under its Privacy Good Research Fund with the aim of stimulating privacy related research by external entities. The conditions included milestones and specific requirements. The Office of the Privacy Commissioner accounted for the related grant expenses when evidence of meeting these milestones had been received from the recipient. All of the milestones were met in relation to these grants in 2022 and so no further payments were required in 2023 (2022 : \$5k).

Lease classification

Determining whether a lease is to be treated as an operating lease or a finance lease requires some judgement. Leases where the lessor effectively retains substantially all the risks and benefits of ownership of the leased items are classified as operating leases.

Other expenses and further information

The total comprehensive revenue and expenses is after charging for the following significant expenses:

	Actual 2023 \$000	Actual 2022 \$000
Fees paid to auditors:		
External audit – current year	50	34
External audit – prior year	14	-
Promotion costs:		
Website expenses	26	55
Privacy Week / Forum	5	16
Other marketing expenses	20	26
Total promotion expenses	51	97
Depreciation and amortisation:		
Furniture and fittings	50	43
Computer equipment	45	51
Office equipment	14	13
Intangibles	164	187
Total depreciation and amortisation	273	294
Rental expense on operating leases	432	427
Contract services	76	90
Other operating expenses:		
Computer maintenance/licences	367	321
Staff travel	97	22
Staff development	65	87
Loss on disposal	1	2
Grant expenditure	-	5
Recruitment	61	58
Utilities	319	253
Other	294	199
Total other operating expenses	1,204	974

Operating leases as lessee

The future aggregate minimum lease payments to be paid under non-cancellable leases are as follows:

	Actual 2023 \$000	Actual 2022 \$000
Not later than one year	432	417
Later than one year and not later than five years	905	1,312
Total non-cancellable operating leases	1,337	1,729

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The Wellington lease will expire in December 2026 and the Auckland lease will expire in December 2025.

A lease incentive was offered as part of the negotiation of the Auckland lease. This is being accounted for in line with PBE IPSAS 13 Leases.

During 2022, the Privacy Commissioner negotiated new agreement for the lease of Zoom Room equipment. The term is for 24 months and will end in October 2024.

The Privacy Commissioner does not have the option to purchase the assets at the end of the lease term.

There are no restrictions placed on the Privacy Commissioner by any of its leasing arrangements.

Note 5: General funds

	Actual 2023 \$000	Actual 2022 \$000
Opening balance	2,446	1,581
Net surplus	151	865
Closing balance	2,597	2,446

Note 6: Cash and cash equivalents

Accounting policy

Cash and cash equivalents include cash on hand, deposits held at call with banks both domestic and international, other short-term, highly liquid investments, with original maturities of three months or less and bank overdrafts.

	Actual 2023 \$000	Actual 2022 \$000
Cash on hand and at bank	111	56
Cash equivalents – on call account	2,278	1,952
Total cash and cash equivalents	2,389	2,008

The carrying value of short-term deposits with maturity dates of three months or less approximates their fair value.

Note 7: Receivables

Accounting policy

Short-term debtors and receivables are recorded at their face value, less an allowance for expected losses.

	Actual 2023 \$000	Actual 2022 \$000
Receivables	82	57
Prepayments	144	158
Total	226	215
Total receivables comprise:		
GST receivable (exchange transaction)	57	53
Other receivables (exchange transaction)	25	4
Total	82	57

The carrying value of receivables approximates their fair value.

Note 8: Property, plant and equipment

Accounting policy

Property, plant and equipment asset classes consist of furniture and fittings, computer equipment, and office equipment.

Property, plant and equipment are shown at cost less any accumulated depreciation and impairment losses.

Depreciation

Depreciation is provided on a straight-line basis on all property, plant and equipment, at a rate which will write off the cost of the assets to their estimated residual value over their useful lives.

The useful lives and associated depreciation rates of major classes of assets have been estimated as follows:

Furniture and fittings	5–7 years
Computer equipment	4 years
Office equipment	5 years

Additions

The cost of an item of property, plant and equipment is recognised as an asset only when it is probable that future economic benefits or service potential associated with the item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

Where an asset is acquired through a non-exchange transaction (at no cost), or for a nominal cost, it is recognised at fair value when control over the asset is obtained.

Costs incurred after initial acquisition are capitalised only when it is probable that future economic benefits or service potential associated with the item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

The costs of day-to-day servicing of property, plant and equipment are recognised in the statement of comprehensive revenue and expenses as they are incurred.

Disposals

Gains and losses on disposals are determined by comparing the proceeds with the carrying amount of the asset. Gains and losses on disposals are included in the statement of comprehensive revenue and expenses.

Impairment of property, plant and equipment

Property, plant and equipment and intangible assets that have a finite useful life are reviewed for impairment whenever events or changes in circumstances indicate that the carrying amount may not be recoverable. An impairment loss is recognised for the amount by which the asset's carrying amount exceeds its recoverable amount. The recoverable amount is the higher of an asset's fair value less costs to sell and value in use.

Value in use is the depreciated replacement cost for an asset where the future economic benefits or service potential of the asset are not primarily dependent on the asset's ability to generate net cash inflows and where the Privacy Commissioner would, if deprived of the asset, replace its remaining future economic benefits or service potential.

If an asset's carrying amount exceeds its recoverable amount, the asset is impaired and the carrying amount is written down to the recoverable amount.

For assets not carried at a revalued amount, the total impairment loss is recognised in the statement of comprehensive revenue and expenses.

Accounting estimates and assumptions

Estimating useful lives and residual values of property, plant and equipment

At each balance date the Privacy Commissioner reviews the useful lives and residual values of its property, plant and equipment. Assessing the appropriateness of useful life and residual value estimates of property, plant and equipment requires the Privacy Commissioner to consider a number of factors such as the physical condition of the asset, expected period of use of the asset by the Privacy Commissioner, and expected disposal proceeds from the future sale of the asset.

An incorrect estimate of the useful life or residual value will impact the depreciation expense recognised in the statement of comprehensive revenue and expenses and carrying amount of the asset in the statement of financial position.

The Privacy Commissioner minimises the risk of this estimation uncertainty by:

- physical inspection of assets
- asset replacement programmes
- review of second-hand market prices for similar assets; and
- analysis of prior asset sales.

The Privacy Commissioner has not made significant changes to past assumptions concerning useful lives and residual values.

Breakdown of property, plant and equipment and further information

	Furniture and fittings \$000	Computer equipment \$000	Office equipment \$000	Total \$000
Cost				
Balance at 1 July 2021	208	221	75	504
Additions	69	86	29	184
Disposals	–	(41)	(16)	(57)
Transfers from Work in Progress	11	–	–	11
Balance at 30 June/1 July 2022	288	266	88	642
Additions	18	17	–	35
Disposals	–	(94)	–	(94)
Balance at 30 June 2023	306	189	88	583
Accumulated depreciation				
Balance at 1 July 2021	20	141	50	211
Depreciation expense	43	51	13	107
Elimination on disposal	–	(40)	(16)	(56)
Balance at 30 June/1 July 2022	63	152	47	262
Depreciation expense	50	45	14	109
Elimination on disposal	–	(93)	–	(93)
Balance at 30 June 2023	113	104	61	278
Carrying amounts				
At 30 June 2022	225	114	41	380
At 30 June 2023	193	85	27	305

There are no restrictions over the title of the Privacy Commissioner's property, plant and equipment, nor are any pledged as security for liabilities.

Capital commitments

The Privacy Commissioner has capital commitments of \$nil as at 30 June 2023. (2022: \$nil).

Note 9: Intangible assets

Accounting policy

Software acquisition

Acquired computer software licenses are capitalised based on the costs incurred to acquire and bring to use the specific software and only when the license covers a period of over 2 years.

Costs associated with maintaining computer software are recognised as an expense when incurred.

Website costs

Costs that are directly associated with the development of interactive aspects of the Office's website are capitalised when they are ready for use.

Costs associated with general maintenance and development of non-interactive aspects of the Office's website are recognised as an expense as incurred.

Amortisation

The carrying value of an intangible asset with a finite life is amortised on a straight-line basis over its useful life. Amortisation begins when the asset is available for use and ceases at the date that the asset is derecognised. The amortisation charge for each period is recognised in the statement of comprehensive revenue and expenses.

The useful lives and associated amortisation rates of major classes of intangible assets have been estimated as follows:

Acquired computer software	2–4 years
Interactive tools	3 years

The software is amortised over the length of the licence.

Impairment

Refer to the policy for impairment of property, plant and equipment in Note 8. The same approach applies to the impairment of intangible assets.

Accounting estimates and assumptions

Estimating useful lives of software assets

The Office's capitalised interactive website tools comprise of a number of interactive website tools and e-learning modules that have been capitalised over the past 6 years. The tools were mainly developed by external providers. These tools have a finite life, which requires the Office to estimate the useful life of the assets.

In assessing the useful lives of these tools, several factors are considered, including:

- the effect of technological change on systems and platforms
- the expected timeframe for the development of replacement systems and platforms.

An incorrect estimate of the useful lives of these assets will affect the amortisation expense recognised in the surplus or deficit, and the carrying amount of the assets in the statement of financial position.

Taking the above into account the Office has estimated a useful life of three years for these interactive tools and there are currently no indicators that the period of use of the tools will be materially different.

Treatment of software-as-a-service arrangements

In April 2021, the IASB's Interpretation Committee issued an agenda decision that clarified the accounting treatment expected for customisation and configuration costs associated with software as a service (SAAS) arrangements.

A detailed review of \$222,894 of assets, previously capitalised and believed to be SAAS related, was undertaken for the year ended 30 June 2022. As a result, most of the assets were determined to not be SAAS related and therefore no adjustment was required. Two remaining assets with a total cost of \$87k were deemed to be SAAS related. Of these, one was fully written down as at 30 June 2022 and the net book value of the remaining asset as at 30 June 2023 is now only \$5k.

Due to the immateriality of the balances identified, no historical accounting adjustments were made in the accounts for the year ended 30 June 2022.

There have been no further software capitalisations in the year to 30 June 2023.

Movements for each class of intangible asset are as follows:

	Acquired software \$000	Interactive tools \$000	Total \$000
Cost			
Balance at 1 July 2021	159	596	755
Additions	–	7	7
Disposals	–	(54)	(54)
Transfers from Work in Progress	–	103	103
Balance at 30 June 2022/ 1 July 2022	159	652	811
Disposals	(67)	–	(67)
Balance at 30 June 2023	92	652	744
Accumulated amortisation			
Balance at 1 July 2021	114	308	422
Amortisation expense	29	158	187
Disposals	–	(53)	(53)
Balance at 30 June 2022/1 July 2022	143	413	556
Amortisation expense	11	153	164
Disposals	(67)	–	(67)
Balance at 30 June 2023	87	566	653
Carrying amounts			
At 30 June and 1 July 2022	16	239	255
At 30 June 2023	5	86	91

There are no restrictions over the title of the Privacy Commissioner's intangible assets, nor are any intangible assets pledged as security for liabilities.

Capital commitments

The Privacy Commissioner has capital commitments of \$nil as at 30 June 2023. (2022: \$nil).

Note 10: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	Actual 2023 \$000	Actual 2022 \$000
Payables under exchange transactions		
Creditors	68	87
Accrued expenses	83	53
Lease incentive	7	7
Total creditors and other payables	158	147

There were no payables under non-exchange transactions (2022 \$nil).

Creditors and other payables are non-interest bearing and are normally settled on 30-day terms, therefore the carrying value of creditors and other payables approximates their fair value.

Note 11: Non-current liabilities

	Actual 2023 \$000	Actual 2022 \$000
Lease incentive	9	16
Total non-current liabilities	9	16

Lease incentive for the Auckland office for the period 1 December 2019 to 30 November 2025 (6-year lease).

Note 12: Employee entitlements

Accounting policy

Employee entitlements that the Privacy Commissioner expects to be settled wholly within 12 months after the end of the reporting period in which the employees render the related service, are measured based on accrued entitlements at current rates of pay.

These include salaries and wages accrued up to balance date and annual leave earned but not yet taken at balance date, expected to be settled within 12 months.

Breakdown of employee entitlements

	Actual 2023 \$000	Actual 2022 \$000
Current employee entitlements are represented by:		
Annual leave	247	249
Total current portion	247	249
Total employee entitlements	247	249

Note 13: Contingencies

There are no known contingencies existing at balance date (2022: \$nil). The Privacy Commissioner used to be subject to “Make Good” clauses in its lease contracts but there are no such clauses included in the current contracts.

Note 14: Related party information

The Privacy Commissioner is a wholly owned entity of the Crown. The Government significantly influences the role of the Privacy Commissioner as well as being its major source of revenue.

Related party disclosures have not been made for transactions with related parties that are within a normal supplier or client/recipient relationship on terms and conditions no more or less favourable than those that it is reasonable to expect the Privacy Commissioner would have adopted in dealing with the party at arm’s length in the same circumstances. Further, transactions with other government agencies (for example, government departments and Crown entities) are not disclosed as related party transactions when they are consistent with the normal operating arrangements between government agencies and undertaken on the normal terms and conditions for such transactions.

There were no other related party transactions.

Key management personnel compensation

	Actual 2023 \$000	Actual 2022 \$000
Total salaries and other short-term employee benefits	1,274	1,178
Full-time equivalent members	4.7	4.4

Key management personnel include all Senior Managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT).

Note 15: Post balance date events

There are no other adjusting events after balance date of such importance that non-disclosure would affect the ability of the users of the financial report to make proper evaluations and decisions.

Note 16: Financial instruments

16A Financial instrument categories

The carrying amounts of financial assets and liabilities in each of the financial instrument categories are as follows:

	2023 \$000	2022 \$000
FINANCIAL ASSETS		
Financial assets measured at amortised cost		
Cash and cash equivalents	2,389	2,008
Receivables (excluding prepayments and taxes receivables)	25	4
Total loans and receivables	2,414	2,012
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	152	140
Total financial liabilities at amortised cost	152	140

Note 17: COVID-19 financial impact assessment

Following the move to the Covid Protection Framework in the previous financial year, December 2021, there have been no further lock-downs affecting the Office in the year to 30 June 2023.

Whilst a small number of staff have still been required to isolate at home during the year, the updated IT infrastructure has enabled staff to work remotely when necessary and there has not been any impact on the delivery of operations across the two Offices.

Some areas of expenditure have increased when compared to the prior year, for example, travel costs, due to the removal of restrictions. No Data and Communications allowances have been paid in 2023 (2022: \$7k) as this was not required.

Appendices | Ngā Tāpiritanga



Appendix A | Tāpiritanga A

Processes and services |

Ngā Tukanga me ngā Ratonga

Investigations and Dispute Resolution

Our Investigations and Dispute Resolution function investigates complaints from the public about interferences with individuals' privacy. It works with parties to achieve fair outcomes using various dispute-resolution techniques.

During an investigation, we assess whether the respondent agency has breached the Privacy Act and if the complainant has suffered harm that requires a remedy, such as an apology or compensation. We can compel agencies to produce documents for our review and meet with complainants. We can't compel complainants or respondents to accept settlement terms and we can't award damages. However, our view is an important indication of whether there's been an interference with privacy.

Advice and advocacy

We provide advice to a range of organisations on the privacy risks of various initiatives. We also offer advice to help organisations mitigate privacy risks.

Our advice is sometimes solicited from agencies that are looking to amend internal policy, and we sometimes proactively provide advice on upcoming legislation. This is generally in the form of submissions to select committees, but we also provide input to Cabinet papers and may brief Cabinet committees in person.

We also engage with the private sector on a variety of projects, such as Privacy Impact Assessments. This is a growing area, with more private-sector organisations managing their privacy risks by engaging with our team early in technology-deployment projects.

Information sharing and matching

A significant portion of our work involves Approved Information Sharing Agreements. These are agreements between government agencies that allow them to share information with one another. We're consulted on these agreements and highlight potential risks.

Information matching involves a comparison of one set of records with another, generally to find records in both sets that belong to the same person. Information matching raises several privacy issues, such as the potential to disclose incorrect date information and the potential to 'automate away' human judgement.

One of the Privacy Commissioner's functions is to require government departments to report on their operation of authorised information matching programmes and, in turn, report to Parliament with an outline of each programme and an assessment of each programme's compliance with the Privacy Act.

Communications and engagement

Our Communications and Engagement team works to raise privacy awareness and engage with stakeholders. It works through many channels, producing material such as:

- Speeches and presentations for the Commissioner.
- Media releases and advisories.
- Blog posts.
- Social media content.
- Case notes.
- Our monthly newsletter.

We also produce guidance on privacy. A key part of this is our e-learning modules. We've worked with education experts to build a suite of online courses covering various aspects of privacy and continue to develop new courses.

We respond to enquiries from journalists and the public via traditional media as well as social media.

Compliance and enforcement

The Compliance and Enforcement team is responsible for identifying and assessing systemic issues and using our compliance tools to get the best privacy outcomes for New Zealanders. The team's work includes enforcing compliance with the Privacy Act and codes of practice, responding to privacy breach notifications from agencies, and applying our full range of compliance and enforcement options as set out in our Compliance and Regulatory Action Framework.

Strategy and insights

The Strategy and Insights team is responsible for understanding trends and developments, both nationally and internationally, that will be relevant in the future. Insights Reports are produced to share this trend intelligence. Using evidence from all OPC's activities, the team helps to prioritise the delivery of work and services accordingly. Following prioritisation, the team monitors the success of the strategies and initiatives put into place and advises the Commissioner on the best way for OPC to achieve its mission. This area also leads OPC's work to engage and partner with Māori.

Appendix B | Tāpiritanga B

Statutory review of information matching provisions

The Privacy Act requires the Commissioner to review the operation of each information matching provision every five years. In these reviews under s 184 the Commissioner recommends whether a provision should continue, be amended, or be cancelled.

This year the Commissioner issued two reports reviewing information matching provisions.

Report by the Privacy Commissioner to the Minister of Justice in relation to a review of the operation of five information matching provisions: Review of statutory authorities for information matching (September 2022):

- Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A.
- Citizenship Act 1977, section 26A.
- Corrections Act 2004, section 181 and Immigration Act 2009, section 294.
- Customs and Excise Act 2018, section 310.
- Immigration Act 2009, section 295.
- Tax Administration Act 1994, Schedule 7 Part C subpart 2 clause 4.

With the exception of the Immigration Act section 295, I considered that the authority conferred by these information matching provisions should be continued without amendment. I committed to reviewing section 295 of the Immigration Act 2009 again in 12 months as it's currently not used. This period was to give the Ministry of Justice time to consider whether the online arrival card system currently being implemented would make this match viable.

Report by the Privacy Commissioner to the Minister of Justice on the Identity Verification Service enabling provision: Electronic Identity Verification Act 2012, s 39 (April 2023)

I considered that the authority conferred by these information matching provisions should be continued without amendment.

Review reports are available on our website: <https://privacy.org.nz/privacy-for-agencies/information-sharing/information-matching-reports-and-reviews>

Changes in information matching programmes

Current programmes

There were 45 information matching programmes in operation, and 11 programmes that were not active.

Inactive programmes

1. The Electoral Commission did not operate its programme of five matches to invite people to enrol under the Electoral Act 1993, s 263B.
 - DIA (Citizenship)/EC Unenrolled Voters
 - DIA (Passports)/EC Unenrolled Voters
 - MSD/EC Unenrolled Voters
 - NZTA (Driver Licence)/EC Unenrolled Voters
 - NZTA (Vehicle Registration)/EC Unenrolled Voters
2. The Ministry of Health did not operate the Publicly Funded Health Eligibility match under the Immigration Act 2009, s 300.
3. The Ministry of Justice did not operate the Fines Defaulters Tracing match with Immigration NZ under s 295 of the Immigration Act 2009.
4. The Ministry of Business, Innovation and Employment did not operate the two matches, to identify unlicensed motor vehicle traders: under the Motor Vehicle Sales Act 2003, s 120 and s 121 with Customs Service; or under the Motor Vehicle Sales Act 2003, s 122 and s 123 with the NZ Transport Agency.
5. The Ministry of Social Development did not operate the Customs/MSD Periods of Residence Match under the Customs and Excise Act 2018, s 309, nor the Netherlands Tax Information Match under the Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003.

Non-compliant programmes

Of the active programmes, nine were not compliant. The issues were all either already known to the Ministry of Social Development (MSD) or identified by it during reviews.

- An enquiry form used for the social welfare reciprocity arrangement with Australia is not deleted when no longer required; MSD is still working on a system fix.
- Birth and death, and name change information used in two programmes is not deleted from the matching system after a successful match. MSD has implemented a temporary fix to mask this data until the system replacement, currently under development, is implemented.
- Letters explaining information matching are not sent for six social welfare reciprocity programmes (those with Canada, Denmark, Greece, Ireland, Guernsey and Jersey, and the United Kingdom). This Notice of Information Matching is intended to be sent when the superannuation arrangement is set up for each client to explain that letters about changes will be sent when changes are made, rather than being sent before any record is adjusted.

A warning was given in relation to this non-compliance in 2022. Either these are all under investigation or remedies are in development. I will continue to monitor this progress and take formal enforcement action if necessary.

New provisions and programmes:

Parliament passed no new information matching provisions during the year.

Information exchanges with the Republic of Korea (South Korea) under a social welfare reciprocity agreement were commenced.





Programmes ceasing:




The Department of Internal Affairs is still working on replacing birth and death and other information matching arrangements with information sharing agreements). We describe programmes' compliance in the following manner:

How we assess programme compliance

Our assessment of a matching programme's compliance is based on the information provided to us by agencies as part of regular reporting, and any other issues drawn to our attention during the reporting period. From time to time we actively seek more detailed evidence of compliance with particular rules.

We describe programmes' compliance in the following manner:

-  **Compliant:** where the evidence we've been provided with indicates that the programme complies with the information matching rules.
-  **Not compliant – minor technical issues:** where reporting has identified practices that are not compliant with the information matching rules, but genuine efforts have been made to implement a compliant programme and the risks to individual privacy are low.
-  **Not compliant – substantive issues:** where reporting has identified practices that are not compliant with the information matching rules or other provisions of the Privacy Act that cannot be considered minor technical issues.
-  **Inactive:** where the programme has not been operated during the year.

Accident Compensation Act 2001, s 246 and Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 41	Compliance
<p>1. IR/ACC Compensation and Levies</p> <p>To confirm income amounts for compensation calculations.</p> <p>Inland Revenue (IR) disclosure to ACC: For self-employed people, IR provides ACC with the full name, contact details, date of birth, IR number, and earnings information. For employers, IR provides ACC with the name, address, IR number, and total employee earnings.</p>	
Accident Compensation Act 2001, s 280	Compliance
<p>2. Corrections/ACC Prisoners</p> <p>To ensure that prisoners do not continue to receive earnings-related accident compensation payments.</p> <p>Corrections disclosure to ACC: Corrections provides ACC with the surname, given names, date of birth, gender, date received in prison, and any aliases of all people newly admitted to prison.</p>	
Accident Compensation Act 2001, s 281	Compliance
<p>3. ACC/MSD Benefit Eligibility</p> <p>To identify individuals whose Ministry of Social Development (MSD) entitlement may have changed because they are receiving ACC payments, and to assist MSD in the recovery of outstanding debts.</p> <p>ACC disclosure to MSD: ACC selects individuals who have:</p> <ul style="list-style-type: none"> • Claims where there have been no payments made to the claimants for six weeks (in case MSD needs to adjust its payments to make up for any shortfall), or • Current claims that have continued for two months since the first payment, or • Current claims that have continued for one year since the first payment. <p>For these people, ACC provides MSD with the full names (including aliases), dates of birth, addresses, IR numbers, ACC claimant identifiers, payment start/end dates, and payment amounts.</p>	

4. BDM (Births)/IR Newborns Tax Number

To enable birth information to be confirmed in order to allocate an IR number to a newborn child.

Births, Deaths, and Marriages disclosure to IR: The information includes the child's full name, sex, citizenship status, and birth registration number. Additionally, the full name, address, and date of birth of both mother and father are provided.

**5. BDM (Births)/MoE Student Birth Confirmation**

To improve the quality and integrity of data held on the National Student Index and reduce compliance costs for students by verifying their details for tertiary education organisations.

BDM disclosure to Ministry of Education: BDM provides names, gender, and date of birth of New Zealand-born citizens.

**6. BDM (Births)/MoH NHI and Mortality Register**

To verify and update information on the National Health Index and to compile mortality statistics.

BDM disclosure to Ministry of Health (MoH): BDM provides child's name, gender, date of birth, place of birth, and ethnicity, and parents' names, occupations, dates of birth, places of birth, address(es), and ethnicities. BDM also indicates whether the baby was stillborn.

**7. BDM/MSD Identity Verification**

To confirm the validity of birth certificates used by clients when applying for financial assistance, and to verify that clients are not on the New Zealand deaths register.

BDM disclosure to MSD: BDM provides birth and death information for the 90 years prior to the extraction date.

The birth details include the full name, gender, date of birth, place of birth, birth registration number, and full name of both mother and father. The death details include the full name, gender, date of birth, date of death, home address, death registration number, and spouse's full name.

Not compliant – minor technical issue – information retained. MSD has implemented a temporary fix and is developing a replacement system.

**8. BDM (Deaths)/GSF Eligibility**

To identify members or beneficiaries of the Government Superannuation Fund (GSF) who have died.

BDM disclosure to GSF: BDM provides information from the New Zealand Deaths Register covering the 12 weeks prior to the extraction date. The information includes the full name at birth, full name at death, gender, date of birth, date of death, place of birth, and number of years lived in New Zealand (if not born in New Zealand).

**9. BDM (Deaths)/INZ Deceased Temporary Visa Holders**

To identify and remove or update the records of people who are deceased from the Immigration New Zealand (INZ) database of overstayers and temporary permit holders.

BDM provides information from the New Zealand deaths register covering the six months prior to the extract date. The information includes the full name at birth, full name at death, gender, birth date, death date, country of birth, and number of years lived in New Zealand.

**10. BDM (Deaths)/IR Deceased Taxpayers**

To identify taxpayers who have died so that IR can close accounts where activity has ceased.

BDM disclosure to IR: BDM provides death information including the full name, gender, date of birth, date of death, home address, death registration number, and spouse's details.

**11. BDM (Deaths)/MoH NHI and Mortality Register**

To verify and update information on the Ministry of Health National Health Index (NHI) and to compile mortality statistics.





BDM disclosure to MoH: BDM provides the full name (including name at birth if different from current name), address, occupation, ethnicity, gender, date of birth, place of birth, date of death, place of death, and cause(s) of death.



Births, Deaths, Marriages, and Relationships Registration Act 2021, s 112 (continued)	Compliance
<p>12. BDM (Deaths)/MSD Deceased Persons</p> <p>To identify current clients who have died so that MSD can stop making payments in a timely manner.</p> <p>BDM disclosure to MSD: BDM provides death information for the week prior to the extraction date. The death details include the full name, gender, date of birth, date of death, home address, death registration number, and spouse's full name.</p>	
<p>13. BDM (Deaths)/NPF Eligibility</p> <p>To identify members or beneficiaries of the National Provident Fund (NPF) who have died.</p> <p>BDM disclosure to NPF: BDM provides information from the New Zealand Deaths Register covering the 12 weeks prior to the extraction date. The information includes the full name at birth, full name at death, gender, date of birth, date of death, place of birth, and number of years lived in New Zealand (if not born in New Zealand).</p>	
<p>14. BDM (Deaths)/NZTA Deceased Driver Licence Holders</p> <p>To improve the quality and integrity of data held on the Driver Licence Register by identifying licence holders who have died.</p> <p>BDM disclosure to NZ Transport Agency (NZTA): BDM provides the death information for the fortnight prior to the extraction date. The death details include the full name (including name at birth if different from current name), gender, date of birth, place of birth, date of death, home address, and death registration number.</p>	
<p>15. BDM (Marriages)/MSD Married Persons Benefit Eligibility</p> <p>To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances.</p> <p>BDM disclosure to MSD: BDM provides marriage information covering the week prior to the extraction date. The marriage details include the full name of each spouse (including name at birth if different from current name), date of birth, address, and registration and marriage dates.</p>	
<p>16. BDM/DIA(Citizenship) Citizenship Application Processing</p> <p>To verify a parent's citizenship status if required for determining an applicant's eligibility for New Zealand citizenship.</p> <p>BDM disclosure to Citizenship (Department of Internal Affairs): Possible matches from the Births, Deaths, and Marriages (relationships) databases are displayed to Citizenship staff as they process each application. These details include the full name, gender, date of birth, place of birth, and parents' full names.</p>	
<p>17. BDM/DIA(Passports) Passport Eligibility</p> <p>To verify, by comparing details with the Births, Deaths, and Marriages registers, whether a person is eligible for a passport, and to detect fraudulent applications.</p> <p>BDM disclosure to Passports (DIA): Possible matches from the Births, Deaths, and Marriages (relationships) databases are displayed to Passports staff as they process each application. The details displayed include the full name, gender, and date of birth.</p>	
<p>18. BDM/MSD Overseas Born Name Change</p> <p>To verify a client's eligibility or continuing eligibility for a benefit where they have legally changed their name in New Zealand and not informed MSD. The programme is also used to identify debtors and suspected benefit fraud.</p> <p>BDM provides name change records from January 2009 to the extract date. The name change details include the full name at birth, former full name, new full name, birth date, residential address, and country of birth.</p> <p>Not compliant – minor technical issue – information retained. MSD has implemented a temporary fix and is developing a replacement system.</p>	

Citizenship Act 1977, s 26A	Compliance
<p>19. DIA (Citizenship)/BDM Citizenship by Birth Processing</p> <p>To enable the Registrar-General to determine the citizenship-by-birth status of a person born in New Zealand on or after 1 January 2006, for the purpose of recording the person's citizenship status on his or her birth registration entry.</p> <p>BDM disclosure to Citizenship (DIA): For birth registration applications, when no parental birth record can be found, a request is transferred electronically to the citizenship unit to be manually checked against the relevant citizenship records. The information supplied includes the child's date of birth, and parents' full names and birth details.</p> <p>Citizenship (DIA) disclosure to BDM: Citizenship responds to these requests by stating either the type of qualifying record found or that qualifying records were not found.</p>	
<p>20. DIA(Citizenship)/DIA(Passports) Passport Eligibility</p> <p>To verify a person's eligibility to hold a New Zealand passport from Citizenship database information.</p> <p>Citizenship (DIA) disclosure to Passports (DIA): Possible matches from the Citizenship database are displayed to Passports staff as they process each application. The possible matches may involve one or more records. The details displayed include the full name, date of birth, country of birth, and date that citizenship was granted.</p>	
<p>21. DIA(Citizenship)/INZ Entitlement to Reside</p> <p>To remove from INZ overstayer records the names of people who have been granted New Zealand citizenship.</p> <p>Citizenship (DIA) disclosure to INZ: Citizenship provides information from the citizenship register about people who have been granted citizenship. Each record the full name, gender, date of birth, country of birth, and citizenship person number.</p>	
Corrections Act 2004, s 180	Compliance
<p>22. Corrections/MSD Prisoners</p> <p>To detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts.</p> <p>Corrections disclosure to MSD: Each day, Corrections sends MSD details about all prisoners who have been admitted, are on muster, or have been released from prison. Details include the name (including aliases), date of birth, prisoner unique identifier, and prison location, along with the incarceration date, parole eligibility date, and statutory release date.</p>	
Corrections Act 2004, s 181 and Immigration Act 2009, s 294	Compliance
<p>23. Corrections/INZ Prisoners</p> <p>To identify prisoners who fall within the deportation provisions of the Immigration Act 2009 as a result of their criminal convictions, or are subject to deportation because their visas to be in New Zealand have expired.</p> <p>Corrections disclosure to INZ: Corrections discloses information about all newly admitted prisoner. The prisoner record includes the prisoner's full name (and known aliases), date of birth, place of birth, gender, and prisoner unique identifier, and the name of the prison facility. Each prisoner's offence and sentence information is also included.</p> <p>INZ disclosure to Corrections: For prisoners who are subject to removal or deportation orders, and who have no further means of challenging those orders, INZ discloses the full names, dates of birth, places of birth, gender, citizenship, prisoner unique identifiers, and immigration status, and details of removal action that INZ intends to take.</p>	

Customs and Excise Act 2018, s 306	Compliance
<p>24. Customs/IR Student Loan Alerts</p> <p>To identify overseas-based borrowers in serious default of their student loan repayment obligations who leave for, or return from, overseas so that IR can take steps to recover the outstanding debt.</p> <p>IR disclosure to Customs: IR provides Customs with the full names, dates of birth, and IR numbers of borrowers in serious default of their student loan obligations.</p> <p>Customs disclosure to IR: Customs provides IR with the borrowers' arrival card information. This includes the borrowers' full names and dates of birth, and the dates, times, and directions of travel, including New Zealand ports and prime overseas ports (last ports of call for arrivals and first ports of call for departures).</p>	
<p>25. Customs/IR Student Loan Interest</p> <p>To detect student loan borrowers who leave for, or return from, overseas so that IR can administer the student loan scheme and its interest-free conditions.</p> <p>IR disclosure to Customs: IR provides Customs with the full names, dates of birth, and IR numbers of student loan borrowers who have loans of more than \$20.</p> <p>Customs disclosure to IR: For possible matches to borrowers, Customs provides the full names, dates of birth, and IR numbers, and the dates, times, and directions of travel.</p>	
Customs and Excise Act 2018, s 307	Compliance
<p>26. Customs/IR Child Support Alerts</p> <p>To identify parents in serious default of their child support liabilities who leave for or return from overseas so that IR can take steps to recover the outstanding debt.</p> <p>IR disclosure to Customs: IR provides Customs with the full names, dates of birth, and IR numbers of parents in serious default of their child support liabilities.</p> <p>Customs disclosure to IR: Customs provides IR with the persons' arrival card information. This includes their full names and dates of birth, and the dates, times, and directions of travel, including New Zealand ports and prime overseas ports (last ports of call for arrivals and first ports of call for departures).</p>	
Customs and Excise Act 2018, s 310	Compliance
<p>27. Customs/Justice Fines Defaulters Alerts</p> <p>To improve the enforcement of fines by identifying serious fines defaulters as they cross New Zealand borders, and to increase voluntary compliance through publicity about the programme targeted at travellers.</p> <p>Justice disclosure to Customs: Justice provides Customs with the full names, dates of birth, gender, and Justice unique identifier numbers of serious fines defaulters for inclusion on the 'silent alerts' or 'interception alerts' list.</p> <p>Customs disclosure to Justice: For each alert triggered, Customs supplies the full name, date of birth, gender, nationality, and presented passport number, along with details about the intended or just completed travel.</p>	

Education and Training Act 2020, Schedule 3 cl 9	Compliance
<p>28. MoE/Teaching Council Registration</p> <p>To ensure teachers are correctly registered (Teaching Council) and paid correctly (Ministry of Education).</p> <p>MoE disclosure to Teaching Council: MoE provides the full name, date of birth, gender, address, school(s) employed at, number of half days worked, registration number (if known), and MoE employee number.</p> <p>Teaching Council disclosure to MoE: The Teaching Council provides the full name, date of birth, gender, address, registration number, registration expiry date, registration classification, and MoE employee number (if confirmed).</p>	
Education and Training Act 2020, Schedule 9 cl 7	Compliance
<p>29. MoE/MSD (StudyLink) Results of Study</p> <p>To determine eligibility for student loans and/or allowances by verifying students' study results.</p> <p>MSD StudyLink disclosure to Ministry of Education (MoE): StudyLink provides MoE with the student's name(s) (in abbreviated form), date of birth, IR number, first known study start date, end date (date of request), known education provider(s) used by this student, and student ID number.</p> <p>MoE disclosure to MSD StudyLink: MoE returns to StudyLink information showing all providers and courses used by the student, course dates, course equivalent full-time student rating, and course completion code.</p>	
Education and Training Act 2020, Schedule 9 cl 8 & 9	Compliance
<p>30. Educational Institutions/MSD (StudyLink) Loans and Allowances</p> <p>To verify student enrolment information to confirm entitlement to allowances and loans.</p> <p>MSD StudyLink disclosure to educational institutions: When requesting verification of a student's course enrolments, MSD StudyLink provides the educational institution with the student's full name, date of birth, MSD client number, and student ID number.</p> <p>Educational institutions' disclosure to MSD StudyLink: The educational institutions return to MSD StudyLink the enrolled students' names, dates of birth, MSD client numbers, student ID numbers, and study details.</p>	
Electoral Act 1993, s 263A	Compliance
<p>31. INZ/EC Unqualified Voters</p> <p>To identify, from immigration records, those on the electoral roll who appear not to meet New Zealand residency requirements, so their names may be removed from the roll.</p> <p>INZ disclosure to the Electoral Commission (EC): INZ provides the full name (including aliases), date of birth, address, and permit expiry date. The type of permit can be identified because five separate files are received, each relating to a unique permit type.</p>	

32. DIA Identity Verification Service (IVS)

To verify identity information provided by an applicant in support of their application for the issuance, renewal, amendment, or cancellation of an electronic identity credential, or to keep the core information contained in an electronic identity credential accurate and up to date.

Births disclosure to IVS: A child's name, gender, date of birth, place of birth, country of birth, citizenship by birth status, marriage date, registration number, mother's name, father's name, since died indicator, and stillborn indicator.

Deaths disclosure to IVS: Name, gender, date of birth, place of birth, date of death, place of death, and age at death.

Marriages disclosure to IVS: Name, date of birth, date of marriage, registration number, country of birth, gender, place of marriage, and spouse's names.

Citizenship disclosure to IVS: Names, gender, date of birth, place of birth, photograph, citizenship person identifier, citizenship certificate number, certificate type, and certificate status.

Passports disclosure to IVS: Names, gender, date of birth, place of birth, photograph, passport person identifier, passport number, date passport issued, date passport expired, and passport status.

Immigration disclosure to IVS: Whether a match is found, client ID number and any of the pre-defined set of identity-related alerts.

**33. Australia (Centrelink)/MSD Change in Circumstances**

For MSD and Centrelink (the Australian Government agency administering social welfare payments) to exchange benefit and pension applications, and changes of client information.

Centrelink disclosure to MSD: When Australian social welfare records are updated for people noted as having New Zealand social welfare records, Centrelink automatically sends updates to MSD, which include the full names, marital status, addresses, bank accounts, benefit status, residency status, income changes, MSD client numbers, and Australian Customer Reference Numbers.

MSD disclosure to Centrelink: MSD automatically sends the same fields of information to Centrelink when New Zealand social welfare records are updated, if a person is noted as having an Australian social welfare record.

Not compliant – minor technical issue.

**34. Canada/MSD Social Welfare Reciprocity**



To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Canada.

Canada disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.

MSD disclosure to Canada: includes full name, date of birth, marital status, address, entitlement information, and MSD client number.

Not compliant – Notice of Information Matching letter advising of process around changes to entitlement is not sent, but adverse action letters advising of actual changes are sent.



Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Denmark) Order 1997	Compliance
<p>35. Denmark/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Denmark.</p> <p>Denmark disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.</p> <p>MSD disclosure to Denmark: Includes full name, date of birth, marital status, address, entitlement information, and MSD client number.</p> <p>Not compliant – Notice of Information Matching letter advising of process around changes to entitlement is not sent, but adverse action letters advising of actual changes are sent.</p>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Hellenic Republic) Order 1993	Compliance
<p>36. Hellenic Republic/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Hellenic Republic.</p> <p>Hellenic Republic disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.</p> <p>MSD disclosure to Hellenic Republic: Includes full name, date of birth, marital status, address, entitlement information, and MSD client number.</p> <p>Not compliant – Notice of Information Matching letter advising of process around changes to entitlement is not sent, but adverse action letters advising of actual changes are sent.</p>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Ireland) Order 1993	Compliance
<p>37. Ireland/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Ireland.</p> <p>Ireland disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.</p> <p>MSD disclosure to Ireland: Includes full name, date of birth, marital status, address, entitlement information, and MSD client number.</p> <p>Not compliant – Notice of Information Matching letter advising of process around changes to entitlement is not sent, but adverse action letters advising of actual changes are sent.</p>	

Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Jersey and Guernsey) Order 1995	Compliance
<p>38. Jersey and Guernsey/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Jersey and Guernsey.</p> <p>Jersey and Guernsey disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.</p> <p>MSD disclosure to Jersey and Guernsey: Includes full name, date of birth, marital status, address, entitlement information, and MSD client number.</p> <p>Not compliant – Notice of Information Matching letter advising of process around changes to entitlement is not sent, but adverse action letters advising of actual changes are sent.</p>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Malta) Order 2013	Compliance
<p>39. Malta/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Malta.</p> <p>Malta disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Maltese Identity Card and Social Security numbers.</p> <p>MSD disclosure to Malta: Includes full name, date of birth, marital status, address, entitlement information, and MSD client number.</p>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003	Compliance
<p>40. Netherlands/MSD Change in Circumstances</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Netherlands.</p> <p>MSD disclosure to the Netherlands: MSD forwards the appropriate application forms to the Netherlands Sociale Verzekeringsbank (SVB). The forms include details such as the full names, dates of birth, addresses, and MSD client numbers.</p> <p>Netherlands disclosure to MSD: SVB responds with the SVB reference number.</p>	
<p>41. Netherlands/MSD General Adjustment</p> <p>To enable the processing of general adjustments to benefit rates for individuals receiving pensions from both New Zealand and the Netherlands.</p> <p>MSD disclosure to the Netherlands: For MSD clients in receipt of both New Zealand and Netherlands pensions, MSD provides the Netherlands SVB with the changed superannuation payment information, the MSD client reference number, and the Netherlands unique identifier.</p> <p>Netherlands disclosure to MSD: SVB advises adjustments to payment rates and the 'holiday pay' bonus.</p>	
Social Security Act 2018, s 380 and Social Security (Reciprocity with the Republic of Korea) Order 2021	Compliance
<p>42. South Korea/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Republic of Korea (South Korea).</p> <p>South Korea disclosure to MSD: includes full name, date of birth, marital status, address, entitlement information, and Korean National Pension Number (or Korean Resident Registration Number).</p> <p>MSD disclosure to South Korea: Includes full name, date of birth, marital status, address, entitlement information, and New Zealand client number.</p>	

Social Security Act 2018, s 380 and Social Security (Reciprocity with the United Kingdom) Order 1990	Compliance
<p>43. United Kingdom/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the United Kingdom (UK).</p> <p>UK disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.</p> <p>MSD disclosure to UK: Includes full name, date of birth, marital status, address, entitlement information, and New Zealand client number.</p> <p>Not compliant – Notice of Information Matching letter advising of process around changes to entitlement is not sent, but adverse action letters advising of actual changes are sent.</p>	
Social Security Act 2018, Schedule 6, cl 13	Compliance
<p>44. MSD/Justice Fines Defaulters Tracing</p> <p>To enable the Ministry of Justice to locate people who have outstanding fines, in order to enforce payment.</p> <p>Justice disclosure to MSD: Justice selects fines defaulters for whom it has been unable to find current addresses from other sources (including the IR/Justice Fines Defaulters Tracing Programme), and sends their full names, dates of birth, and data matching reference numbers to MSD.</p> <p>MSD disclosure to Justice: For matched records, MSD returns the last known residential addresses, postal addresses, residential, cell-phone and work phone numbers, and the unique identifier originally provided by Justice.</p>	
Social Security Act 2018, Schedule 6, cl 15	Compliance
<p>45. Justice/MSD Warrants to Arrest</p> <p>To enable MSD to suspend or reduce the benefits of people who have outstanding warrants to arrest for criminal proceedings.</p> <p>Justice disclosure to MSD: Justice provides MSD with the full names (and alias details), dates of birth, addresses, Justice unique identifiers, and warrant to arrest details.</p>	
Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 43	Compliance
<p>46. IR/Justice Fines Defaulters Tracing</p> <p>To enable the Ministry of Justice to locate people who have outstanding fines, in order to enforce payment.</p> <p>Justice disclosure to IR: Justice selects fines defaulters for whom it has been unable to find current addresses, and sends the full names, dates of birth, and data matching reference numbers to IR.</p> <p>IR disclosure to Justice: For matched records, IR supplies the current address and all known telephone numbers for a person, the name, address, and contact numbers of the person's employer or employers, and the unique identifier originally provided by Justice.</p>	

Appendix C | Tāpiritanga C Independent Auditor's Report | Pūrongo Kaitātāri Kaute Motuhake

To the readers of the Privacy Commissioner's financial statements and performance information for the year ended 30 June 2023

The Auditor-General is the auditor of the Privacy Commissioner. The Auditor-General has appointed me, Melissa Collier, using the staff and resources of Deloitte Auckland, to carry out the audit of the financial statements and the performance information, including the performance information for appropriations, of the Privacy Commissioner on his behalf.

Opinion

We have audited:

- the financial statements of the Privacy Commissioner on pages 43 to 63, that comprise the statement of financial position as at 30 June 2023, the statement of comprehensive revenue and expenses, statement of changes in equity and statement of cash flows for the year ended on that date and the notes to the financial statements including a summary of significant accounting policies and other explanatory information; and
- the performance information which reports against the Privacy Commissioner's statement of performance expectations for the year ended 30 June 2023 on pages 8 to 22 and 32 to 42.

In our opinion:

- the financial statements of the Privacy Commissioner:
 - present fairly, in all material respects:
 - its financial position as at 30 June 2023; and
 - its financial performance and cash flows for the year then ended; and
 - comply with generally accepted accounting practice in New Zealand in accordance with the Public Benefit Entity Standards Reduced Disclosure Regime; and
- the Privacy Commissioner's performance information for the year ended 30 June 2023:
 - presents fairly, in all material respects, for each class of reportable outputs:
 - its standards of delivery performance achieved as compared with forecasts included in the statement of performance expectations for the financial year; and
 - its actual revenue and output expenses as compared with the forecasts included in the statement of performance expectations for the financial year;
 - presents fairly, in all material respects, for the appropriations:
 - what has been achieved with the appropriations; and
 - the actual expenses or capital expenditure incurred as compared with the expenses or capital expenditure appropriated or forecast to be incurred; and
 - complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 31 October 2023. This is the date at which our opinion is expressed.

The basis for our opinion is explained below. In addition, we outline the responsibilities of the Privacy Commissioner and our responsibilities relating to the financial statements and the performance information, we comment on other information, and we explain our independence.

Basis for our opinion

We carried out our audit in accordance with the Auditor-General's Auditing Standards, which incorporate the Professional and Ethical Standards and the International Standards on Auditing (New Zealand) issued by the New Zealand Auditing and Assurance Standards Board. Our responsibilities under those standards are further described in the Responsibilities of the auditor section of our report.

We have fulfilled our responsibilities in accordance with the Auditor-General's Auditing Standards.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Responsibilities of the Privacy Commissioner for the financial statements and the performance information

The Privacy Commissioner is responsible for preparing financial statements and performance information that are fairly presented and comply with generally accepted accounting practice in New Zealand. The Privacy Commissioner is responsible for such internal control as it is necessary to enable the Privacy Commissioner to prepare financial statements and performance information that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements and the performance information, the Privacy Commissioner is responsible for assessing the Privacy Commissioner's ability to continue as a going concern. The Privacy Commissioner is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting, unless there is an intention to merge or to terminate the activities of the Privacy Commissioner, or there is no realistic alternative but to do so.

The Privacy Commissioner's responsibilities arise from the Crown Entities Act 2004 and the Public Finance Act 1989.

Responsibilities of the auditor for the audit of the financial statements and the performance information

Our objectives are to obtain reasonable assurance about whether the financial statements and the performance information, as a whole, are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion.

Reasonable assurance is a high level of assurance, but is not a guarantee that an audit carried out in accordance with the Auditor-General's Auditing Standards will always detect a material misstatement when it exists. Misstatements are differences or omissions of amounts or disclosures, and can arise from fraud or error. Misstatements are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of readers, taken on the basis of these financial statements and the performance information.

For the budget information reported in the financial statements and the performance information, our procedures were limited to checking that the information agreed to the Privacy Commissioner's statement of performance expectations.

We did not evaluate the security and controls over the electronic publication of the financial statements and the performance information.

As part of an audit in accordance with the Auditor-General's Auditing Standards, we exercise professional judgement and maintain professional scepticism throughout the audit. Also:

- We identify and assess the risks of material misstatement of the financial statements and the performance information, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- We obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Privacy Commissioner's internal control.
- We evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Privacy Commissioner.
- We evaluate the appropriateness of the reported performance information within the Privacy Commissioner's framework for reporting its performance.

- We conclude on the appropriateness of the use of the going concern basis of accounting by the Privacy Commissioner and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Privacy Commissioner's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements and the performance information or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Privacy Commissioner to cease to continue as a going concern.
- We evaluate the overall presentation, structure and content of the financial statements and the performance information, including the disclosures, and whether the financial statements and the performance information represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with the Privacy Commissioner regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

Our responsibilities arise from the Public Audit Act 2001.

Other information

The Privacy Commissioner is responsible for the other information. The other information comprises the information included on pages 2 to 7, 23 to 31, and 64 to 79 but does not include the financial statements and the performance information, and our auditor's report thereon.

Our opinion on the financial statements and the performance information does not cover the other information and we do not express any form of audit opinion or assurance conclusion thereon.

In connection with our audit of the financial statements and the performance information, our responsibility is to read the other information. In doing so, we consider whether the other information is materially inconsistent with the financial statements and the performance information or our knowledge obtained in the audit, or otherwise appears to be materially misstated. If, based on our work, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Independence

We are independent of the Privacy Commissioner in accordance with the independence requirements of the Auditor-General's Auditing Standards, which incorporate the independence requirements of Professional and Ethical Standard 1: *International Code of Ethics for Assurance Practitioners (including International Independence Standards) (New Zealand) (PES 1)* issued by the New Zealand Auditing and Assurance Standards Board.

Other than in our capacity as auditor, we have no relationship with, or interests, in the Privacy Commissioner.



Melissa Collier
Deloitte Auckland

On behalf of the Auditor-General
Auckland, New Zealand





Privacy Commissioner
Te Mana Mātāpono Matatapu

Published by the Office of the Privacy Commissioner
PO Box 10094
Wellington
215 Lambton Quay
Wellington 6011
www.privacy.org.nz

© 2023 The Privacy Commissioner
ISSN 1179-9838 (Print)
ISSN 1179-9846 (Online)