A11

Privacy Commissioner
Te Mana Mātāpono Matatapu

Annual Report
2025/26

Annual Report of the Privacy Commissioner

for the year ended 30 June 2026

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

The Minister of Justice

I submit my report as Privacy Commissioner for the year ended 30 June 2026.



Michael Webster CVO
Privacy Commissioner
30 October 2026

© 2026 Office of the Privacy Commissioner. This work is licensed under the Creative Commons Attribution 4.0 International license. In essence, you are free to copy, distribute and adapt the work, as long as you attribute the work to the Office of the Privacy Commissioner and abide by the other license terms. To view a copy of this license visit: https://creativecommons.org/licenses/by/4.0/

Contents

2 Introduction from the Privacy Commissioner

5 Statement of responsibility

6 We are committed to promoting privacy

7 2025/26: privacy in numbers

8 Our strategic framework for 2025/26

9 Tuitui kākahu, tuitui tāngata

10 The privacy system is broad and challenging

11 Privacy benefits all of New Zealand

13 New Zealand needs Privacy Act modernisation

14 Our funding

15 We undertake a wide range of functions

16 We focused on three key things in 2025/26

17 Strategic objectives progress | Te kauneke ki ngā whāinga rautaki

18 Our progress towards our objectives and privacy outcomes

19 Objective 1: We will work in partnership with Māori to take a te ao Māori perspective on privacy

25 Objective 2: We will engage and empower people and communities who are more vulnerable to serious privacy harm

30 Objective 3: We will set clear expectations to provide agencies with greater certainty about their responsibilities

35 Objective 4: We will promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm

42 Office and functions | Te tari me āna mahi

43 Independence and other interests

43 Reporting

43 Staff

44 Statutory remuneration disclosures

44 Employees' remuneration

45 EEO Profile

46 Finance and performance | Pūrongo whakahaere pūtea me ngā tutukitanga

47 Statement of performance

48 PBE FRS 48 Service performance reporting

49 Statement specifying comprehensive income

50 Cost of service statement

52 Performance against statements of service performance

- 52 Function 1: Strategy and Insights
- 53 Function 2: Communications and Education
- 54 Function 3: Compliance and Enforcement
- 55 Function 4: Policy and Advocacy
- 56 Function 5: Investigations and Dispute Resolution

57 Statement of accounting policies

59 Statement of comprehensive revenue and expenses

60 Statement of changes in equity

61 Statement of financial position

62 Statement of cash flows

63 Notes to the financial statements

73 Appendix | Ngā Tāpiritanga

Introduction from the Privacy Commissioner

Privacy is precious. Privacy breaches cause real harm to thousands of New Zealanders a year. This harm can take many forms. It could be emotional hurt arising from intimate information being made public. Or it could be a direct financial loss as the privacy breach was a part of a scam. A privacy breach might also lead to physical harm, if your location became known to the wrong people.

Three years ago, I set for my Office the purpose of making privacy a core focus for agencies. We do this not only to protect the privacy of individuals, but because we believe that privacy enables agencies to achieve their own objectives – whether that is turning a profit or providing a social service. Privacy is also an important safeguard of our free and democratic society, an important point as our country heads to the polls.

We operate in a challenging environment. The volume and complexity of privacy breaches is increasing as individuals and agencies use and share more personal information. This year provided a clear example of the situation. On the first of January, Manage My Health notified my Office that an overseas hacker had accessed the personal information of over 99,000 New Zealanders who were spread across hundreds of medical centres.

New Zealanders appreciate the privacy challenges we are facing. Our annual privacy survey of 1,300 New Zealanders again found that 82% wanted more control and choice over the collection and use of their personal information, but that only 46% felt in control of their data privacy. Three quarters of our respondents also supported strengthening the Privacy Act 2020 in a variety of different ways, including through strengthening the compliance and enforcement powers available to my Office.

I urge our companies, government agencies, councils and not-for-profits to regard privacy not as an “either/or”, but as an “and” or a “while”. You can do privacy well and make a profit. You can provide your clients with the services they need while protecting their privacy rights. You can adopt biometric and artificial intelligence technologies while respecting personal information. New Zealanders will support agencies who respect privacy: two-thirds of our survey respondents state they would consider changing service providers over poor privacy and security practices.

This Annual Report provides an opportunity to reflect on the achievements of my Office this year and the progress we are making.

A positive sign of progress is that our privacy surveys are indicating a small but consistent increase in New Zealanders’ awareness of their privacy right to access their personal information held by agencies. However, I must also caution that the Act needs urgent strengthening given the major privacy breaches, such as the Manage My Health breach, that we now see every year.

Like other agencies, my Office is having to rigorously prioritise how it applies its resources. The Office is currently going through a change exercise focused on reducing our expenditure, while ensuring we are configured in the best way possible to deliver on our strategic direction, purpose, and objectives. As a part of our prioritisation, we changed the way we provide our public enquiries service. We moved away from providing a bespoke public enquiries service and instead now focus on providing a one-to-many self-help service that leverages our website content.

Above all, this Annual Report is a chance for me to acknowledge the work and achievements of my staff that are driving us towards our four objectives:

1. Work in partnership with Māori to take a te ao Māori perspective on privacy.
2. Engage and empower people and communities who are more vulnerable to serious privacy harm.
3. Set clear expectations to provide agencies with greater certainty about their responsibilities.
4. Promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm.

Our achievements this year

Underpinning our achievements is a passion for protecting the privacy of New Zealanders, matched with a pragmatic and constructive approach to the opportunities and challenges that agencies are navigating.

Just some of the highlights of our work this year were:

- Receiving and processing extremely high levels of privacy complaints, with 1,644 received from individuals and in many cases finding they had experienced harm from privacy breaches. An investigation into a large representative complaint involving more than 1,600 affected individuals was completed.
- Releasing a large amount of guidance on how agencies can protect the privacy and safety of children and young people. This was supported by the Privacy Commissioner engaging with public sector agencies around information sharing where there are concerns about the wellbeing or safety of a child or young person.
- Supporting the commencement of the new Information Privacy Principle 3A in the Act with comprehensive guidance and supporting amendments to the codes of practices. We also created a short video on the new principle and presented to a variety of industry bodies and forums.
- Receiving 133 requests for speeches and presentations, and our staff spoke to a diverse range of businesses, peak industry bodies, government agencies, health providers, churches, schools and not for profit organisations.
- Hosting the Sir Bruce Slane Memorial Lecture, in honour of New Zealand's first Privacy Commissioner, with Justice Christian Whata (Ngāti Pikiao and Ngāti Tamateatūtahi – Kawiti of Te Arawa) speaking about the tapu of privacy and viewing privacy through a tikanga lens.
- Continuing our work with Te Ranga Tautiaki, our Māori reference panel, which provides us with an opportunity to receive expert advice on te ao Māori perspectives on our work programme.
- Receiving 2,231 privacy breach notifications, doubling last year's volume due to the many agencies related to the Manage My Health and MediMap cybersecurity breaches. We commenced an Inquiry into the Manage My Health breach, and completed the first phase in the 2025/26 year.

- Making 14 submissions to select committees to ensure privacy is being considered in the Government's legislative programme and petitions from New Zealanders. A major submission for us was stating our clear opposition to the Policing Amendment Bill, which authorises the New Zealand Police to record images and sounds and collect personal information, including for intelligence purposes, without including appropriate safeguards.
- Intervening in a Court of Appeal case considering the lawfulness of New Zealand Police using automatic number plate recognition, focusing on the privacy implications of this technology.
- Completing our website redevelopment in-house, which simplified our website structure and increased accessibility, and simplifying and improving the 650 questions in our Ask Us knowledge base. We supported these efforts through ensuring our privacy rights material is available in Easy Read, sign language, Braille, and in six new languages.
- Hosting Privacy Week 2026, where over 5,500 people watched 18 free webinars on the theme of 'Foundations of the Future', including topics such as AI.
- Contributing to discussions around regulatory options to incentivise the protection of personal information and strengthening compliance with good privacy practice.

Our year has been busy, but successful. I want to thank all of my staff, who have made all the above possible.

I look forward to what we will achieve over the coming year.



Michael Webster CVO
Privacy Commissioner

Statement of responsibility

Under the Crown Entities Act, 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 2026.



Michael Webster CVO
Privacy Commissioner
30 October 2026



Emma Boddy
General Manager
30 October 2026

We are committed to promoting privacy



Michael Webster CVO
Privacy Commissioner

Michael was appointed as Privacy Commissioner in July 2022. Prior to his appointment he was the Secretary of the Cabinet and Clerk of the Executive Council of New Zealand, a position he held since March 2014.

Ko Rangitīkei 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



Liz MacPherson
Deputy Privacy Commissioner

Liz was appointed as the first statutory Deputy Privacy Commissioner in November 2021. Liz first joined the Office of the Privacy Commissioner in April 2020 and previously held several Deputy Chief Executive roles before being appointed to the position of Government Statistician.

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 ināianei

Ko te Komihana Tuarua ahau

Ko Liz MacPherson tōku ingoa

2025/26: privacy in numbers



1. The large increase in serious privacy breaches during 2025/26 arose from two separate cybersecurity breaches affecting 1,222 health agencies (the Manage My Health and MediMap breaches). More information is available later in this Annual Report. The figure excluding the 1,222 health agencies is 488.
2. Due to changes made to our enquiries function in 2025/26, these numbers are for the period 1 July 2025 to 30 April 2026. More information is available later in this Annual Report.

Our strategic framework for 2025/26

Our system outcomes



- Individuals are more confident that their privacy is protected.
- Agencies can better achieve their own objectives through respecting the privacy rights of New Zealanders.
- The right to privacy and the protection of personal information is valued in New Zealand.

Our purpose

We ensure privacy is a core focus for agencies in order to protect the privacy of individuals, enable agencies to achieve their own objectives, and safeguard a free and democratic society.

Our objectives



- We work in partnership with Māori to take a Te Ao Māori perspective on privacy.
- We engage and empower people and communities who are more vulnerable to serious privacy harm.
- We set clear expectations to provide agencies with greater certainty about their responsibilities.
- We promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm.

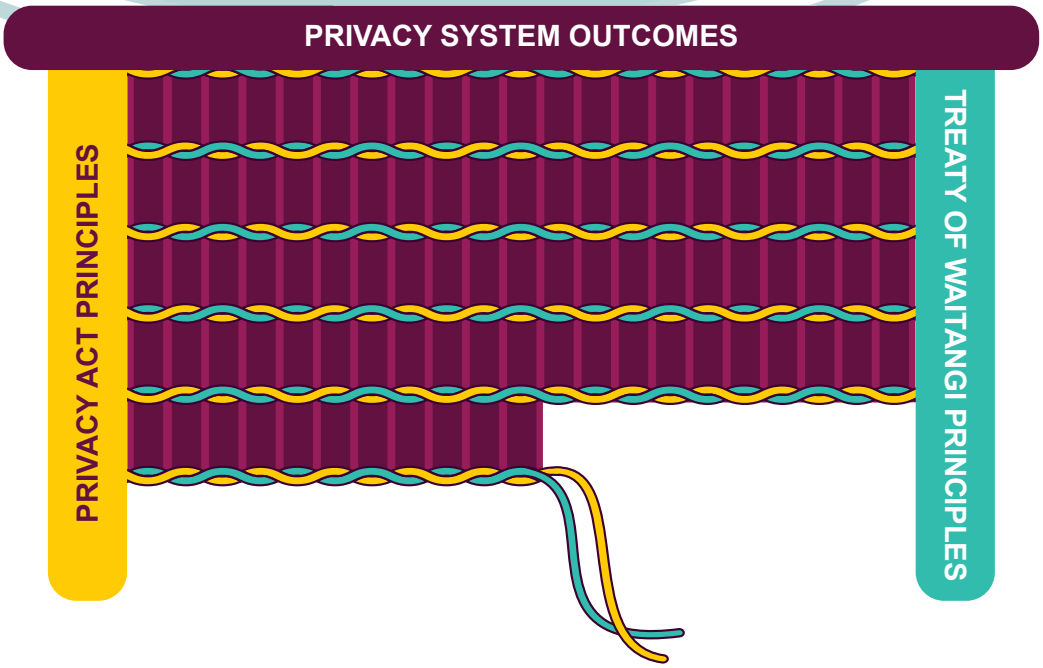
Our functions

- Communication and Education
- Compliance and Enforcement
- Policy and Advocacy
- Investigations and Dispute Resolution
- Strategy and Insights

Our values

Respect + Integrity + Independence + Innovation + Excellence

Tuitui kākahu, tuitui tāngata



The weaving of a cloak, the weaver of people

Our Office is increasingly expected to have a strong understanding and capabilities related to the Treaty of Waitangi / Te Tiriti o Waitangi, tikanga Māori and te ao Māori. In addition, the Act requires the Privacy Commissioner to take account of these perspectives in delivering on the Office's functions. We recognise that to be an effective privacy regulator, we need to engage effectively with Māori, and to identify and respond to te ao Māori perspectives on privacy.

Tuitui kākahu, tuitui tāngata is a whakataukī that speaks to the process of weaving a kākahu or traditional Māori cloak and aligns that to the weaving of people. It is a whakataukī that works well in describing the privacy system, the role of our Office, and the place of the Treaty of Waitangi principles. This includes:

- tiaki – protecting and safeguarding the privacy of all New Zealanders
- taunaki – supporting the aspiration of rangatiratanga as expressed by Māori over their taonga, their data, and their privacy
- tūhono – partnering with Māori.

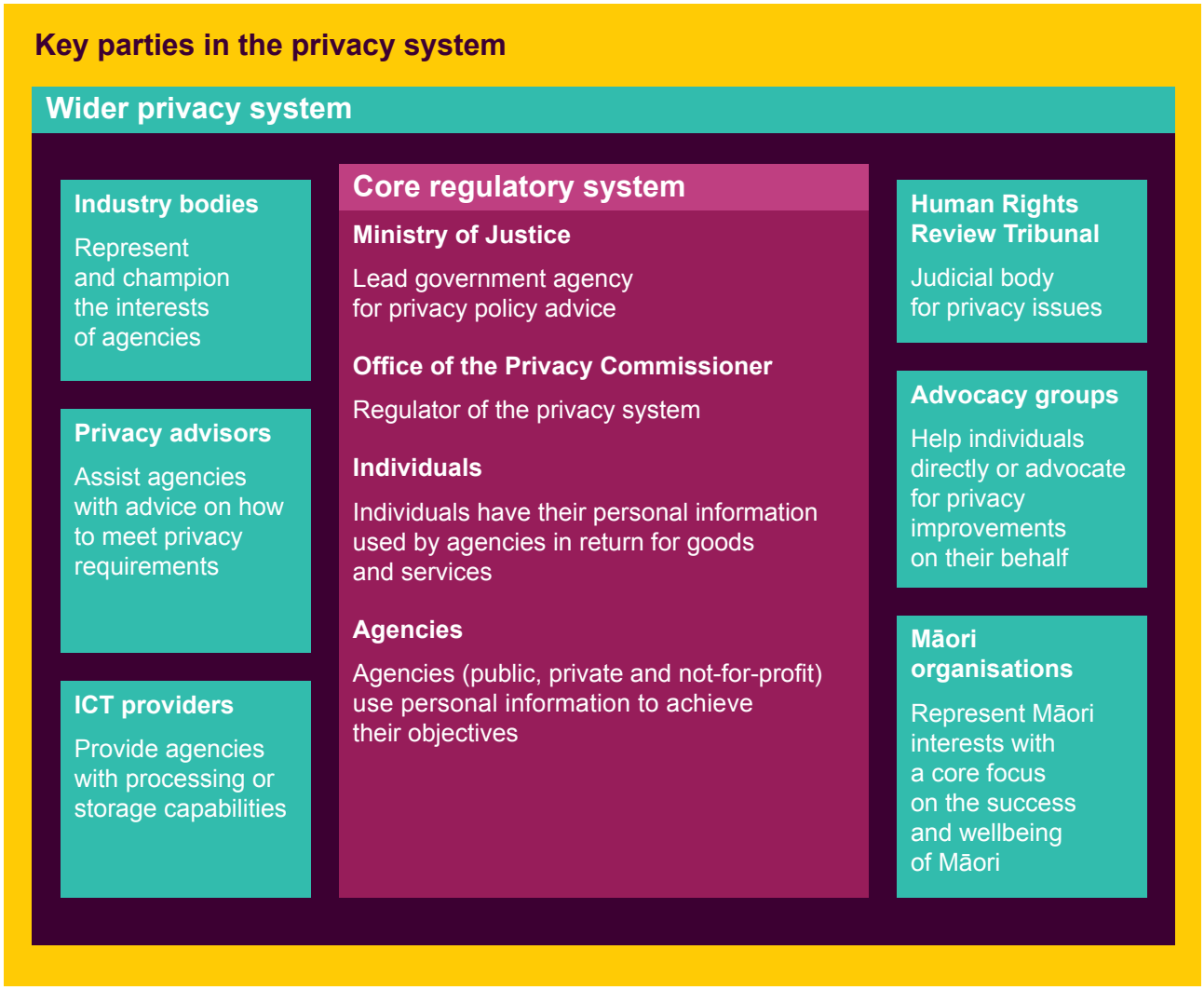
Tuitui kākahu, tuitui tāngata describes the process of weaving and the completion of the garment, or cloak that can then be used by individuals, whānau, hapū, iwi, and Māori to protect their privacy.

This whakataukī represents how the principles of the Treaty of Waitangi and the Act work together to achieve the outcomes of the privacy system.

The privacy system is broad and challenging

We are the regulator of the privacy system – the flows of personal information between individuals and agencies throughout New Zealand. The figure below illustrates the breadth of the privacy system.

The privacy system is a challenging environment to regulate. There are rapid technological changes and a keenness to use technologies such as facial recognition and AI. Our regulated sector is very broad, extending to nearly the entire public, private and not-for-profit sectors. Good privacy practice requires every agency to consider their specific situation, and many have a low understanding about how to manage privacy well.



Privacy benefits all of New Zealand

Our purpose is ‘ensuring that privacy is a core focus for agencies’ as we believe it’s the best way to improve the outcomes of the privacy system. Our interventions are designed to drive improvements to the privacy understanding and capabilities of agencies and to increase the priority and importance of privacy in their decision making.

Our indicators on the performance of the privacy system and privacy outcomes are outlined in the section, ‘Progressing toward our objectives and privacy outcomes’.

The privacy system contributes to three important outcomes for New Zealand.

1

Individuals are more confident that their privacy is protected

When people trust that their personal information will be treated as a taonga, it gives them confidence in an agency.

Good privacy practices reduce the likelihood of a breach happening, and if it does occur, they reduce the harms caused by privacy breaches, whether emotional, reputational, financial, or physical. In 2025/26, when we helped settle a privacy complaint with a financial settlement, the average settlement amount was over $8,000. When the Human Rights Review Tribunal has considered privacy cases this year and determined there should be a financial settlement, the average settlement amount for emotional harm or injury to feelings was approximately $20,000.



Good privacy practices reduce the likelihood of a breach happening, and if it does occur, they reduce the harms caused by privacy breaches.

2

Agencies can better achieve their own objectives through respecting the privacy rights of New Zealanders

Agencies use the personal information that people give to them to deliver goods or services, either for profit or as a public service.

Privacy breaches create high costs to agencies both in remedying what went wrong and, in some cases, reimbursing customers. It can also impact the ability of the business to deliver products or services, as important data may have been lost, and there could be a loss of existing customers or clients. In our 2026 survey of New Zealanders' attitudes to privacy, 66% of respondents said they would likely change service providers if they heard that their provider had poor privacy and security practices.



66%

OF RESPONDENTS SAID THEY WOULD LIKELY CHANGE SERVICE PROVIDERS IF THEY HEARD THAT THEIR PROVIDER HAD POOR PRIVACY AND SECURITY PRACTICES.

3

The right to privacy and the protection of personal information is valued in New Zealand

The outcomes of the privacy system extend beyond the interactions of individuals and agencies.

Collectively, a society that values privacy and personal information is one where its people can have greater trust in government and institutions because they know that the information that is precious to them will be well treated. This trust helps drive better outcomes by encouraging engagement in democratic and consultation processes, helping to inform the design of effective services, and tackling complex problems. This trust is especially important for whānau, hapū, and iwi in achieving their aspirations for equitable outcomes and data sovereignty. We contribute to this trust through our statutory independence that provides the public with a 'watch dog' who advocates on their behalf.



Collectively, a society that values privacy and personal information is one where its people can have greater trust in government and institutions.

New Zealand needs Privacy Act modernisation

The need for change is increasingly urgent

Based upon Law Commission recommendations from 2011, the Act is increasingly outdated and insufficient. In particular, the Act provides insufficient incentives for many agencies to understand or meet basic privacy requirements, leading to significant non-compliance that is difficult for us to address.

The New Zealand public supports the need for Act reform. In our 2026 survey of over 1,300 New Zealanders, approximately 70% of those surveyed considered that the Privacy Commissioner should have the power to audit the privacy practices of agencies, to issue small infringement fines for a privacy breach, and the power to ask Courts to issue large fines for serious privacy breaches.

There is even stronger support for new privacy rights, with over 80% of those surveyed supporting the following being added to the Act:

- a right to request the erasure of their personal information if it is no longer required
- being told in advance if an organisation will use computer algorithms or AI to make decisions
- requiring companies to meet security requirements if they store or process personal information for other organisations
- requiring organisations to document how they meet the requirements of the Act.

During 2026 there were indications that the Government will be considering potential modernisation of the Act. The New Zealand Cyber Security Action Plan 2026–2027 states that the Ministry of Justice will be providing advice on options to incentivise the protection of personal information from cyber threats, such as introducing a civil pecuniary penalty regime.

The specific amendments we propose to the Act

We continue to recommend a specific set of amendments to the Government that would further modernise it and strengthen privacy outcomes. They include:

1. Empowering New Zealanders to better protect themselves with new rights, such as a ‘right to erasure’ that would provide individuals with the right to ask agencies to delete their personal information.
2. Establishing strong incentives for agencies to take privacy seriously through establishing a new and significantly stronger penalty regime.
3. Requiring agencies to be able to demonstrate how they meet their privacy requirements, such as the privacy management programmes recommended by the OECD.
4. Providing New Zealanders with stronger protections for automated decision making, which can have issues with inaccurate predictions, discrimination, unexplainable decisions and a lack of accountability.

Our funding

The recent history of our non-departmental appropriation within Vote Justice is outlined below.

Year	Operating grant from the Ministry of Justice ($000)	Note
2021/22	7,392	
2022/23	7,392	
2023/24	8,171	Budget 2023 funding increases to support compliance and enforcement
2024/25	7,640	Budget 2024 cost savings decrease
2025/26	7,641	
2026/27	7,641	

New levy funding under the Customer and Product Data Act 2025

The Customer and Product Data Act 2025 (the CPD Act) empowers New Zealanders to authorise businesses to transfer their information to another business in a specified format. The Government has prescribed the banking sector as the first sector covered by the CPD Act, with the electricity sector likely to follow.

Our Office has new responsibilities as the privacy regulator of the CPD Act that have been designed to align with and complement our own Act. These responsibilities include investigating complaints and taking compliance action in relation to privacy related breaches. As privacy and public trust will be essential to the sharing of customer information and the success of the CPD Act, the Privacy Commissioner will promote public understanding and trust in the personal information protections supporting the transfer of customer information.

This year was the first period for which our Office received levy funding to meet our new responsibilities. A total of $180,000 was received in 2025/26. More information on this expenditure is available in Note 1 in the section ‘Notes to the financial statements’.

We undertake a wide range of functions

The functions outlined here are from our Statement of Intent 2023–2027. Our new Statement of Intent 2026–2030 makes changes to these functions, including through increasing the prominence of our guidance activities.

Strategy and Insights

- Using intelligence obtained from our activities across our Office to identify domestic trends and emerging strategic issues.
- International insights on emerging privacy issues.
- Understanding new trends globally and prioritising delivery of services accordingly.
- Monitoring the success of new initiatives and strategies introduced.

Communication and Education

- Guidance and education to empower New Zealanders to exercise their privacy rights and agencies on their responsibilities and obligations under the Act.
- Improving digital services channels, including the website and education and guidance tools.
- Commenting on issues of public and media interest.
- Engagement focused on understanding those parts of society more vulnerable to serious privacy harm.

Compliance and Enforcement

- Receiving breach notifications and following up with agencies on those likely to cause serious harm.
- Issuing guidance to agencies reporting a non-serious privacy harm or risk.
- Proactively identifying and investigating systematic issues for possible intervention.
- Setting expectation with agencies about privacy practices and, where necessary, compliance orders to address systematic issues.
- Applying the Compliance and Regulatory Action Framework.

Policy and Advocacy

- Providing clear expectations for agencies, whether through information, guidance or codes of practices.
- Providing advice to the government on emerging and new legislation and policy proposals, applying the principles of necessity and proportionality.
- Supporting responsible information sharing including the facilitation of Approved Information Sharing Agreements (AISAs) to assist public agencies to operate more effectively and efficiently.
- Treaty and te ao Māori analysis incorporated in policy work as necessary.

Investigations and Dispute Resolution

- Investigating privacy complaints made under the Act and referring appropriate complaints to the Director of Human Rights Proceedings for consideration.
- Taking a dispute resolution approach where possible and focusing on settlement.
- Issuing access directions where appropriate.

We focused on three key things in 2025/26

In our third year under the Statement of Intent 2023–2027 we pursued three key areas of strategic focus.[3] Our accomplishments related to these areas are in the Objectives section of this report.

Provide guidance and develop processes to support the implementation of legislative and regulatory privacy initiatives

During the year there were significant initiatives that required strong supporting guidance and processes. Parliament enacted the Privacy Amendment Act 2025, which introduced the new Information Privacy Principle 3A about notifying individuals if their personal information has been collected indirectly. Our Office also issued the Biometric Processing Privacy Code 2025, which strengthened the privacy protections provided to biometric information like facial recognition or fingerprints.

Supporting these initiatives with clear guidance helps provide agencies with a clearer understanding of the new requirements and how they apply to them.

Engage with agencies to build their privacy capability and empower New Zealanders to assert their privacy rights

We understand that agencies need clear advice and guidance from us so that they can do privacy well. This is why we have comprehensive guidance on how agencies can do privacy well: Poupou Matatapu. During the year our focus was on publishing detailed guidance on specific topics and giving speeches and presentations to agencies throughout New Zealand.

We also promote New Zealanders' understanding of their privacy rights to provide them with more control over their personal information. New Zealanders using their privacy rights can motivate agencies to better care for their personal information.

Focus our activities on the technological and digital innovations being adopted by organisations and businesses

New Zealanders expect their privacy regulator to understand and respond to changes. This includes the widespread adoption of AI tools and the retail sector's use of technology to respond to theft and safety issues. Focusing our activities on these innovations helps reduce privacy harms while also supporting agencies to achieve their own objectives.

An important aspect of our work has been advocating for amendments to the Act that would ensure privacy regulation that is fit-for-purpose in a world increasingly powered by AI.

3. These areas were set in the *Statement of Performance Expectations 1 July 2025 to 30 June 2026*.

Strategic objectives progress

Te kauneke ki ngā whāinga rautaki

Our progress towards our objectives and privacy outcomes

Our strategic objectives have been set with the ambition of achieving them over the lifespan of our 2023–2027 Statement of Intent. The objectives will drive us toward being an effective modern privacy regulator who makes privacy a core focus for agencies.

The following sections outline the scope of each objective, what we have achieved so far and the challenges we face. We also include key performance information for the indicators that relate to privacy system outcomes and our objectives.

Measuring privacy outcomes is difficult due to the intangible nature of privacy and because our Office only sees a small part of the personal information flows within New Zealand. This means that significant observable operational volumes, such as privacy complaints from individuals, cannot by themselves be used as an indicator of privacy outcomes. For example, an increase in privacy complaints by individuals could be viewed as either an increase in privacy harm or more people being aware of their privacy rights. With these complexities in mind, we have identified some proxy indicators for privacy outcomes.



...an increase in privacy complaints by individuals could be viewed as either an increase in privacy harm or more people being aware of their privacy rights.



Objective 1:
We will work in partnership with Māori to take a te ao Māori perspective on privacy

This is an Office-wide objective that all our functions support.

Building our te ao Māori capability enables us to provide more culturally appropriate services and better connect with Māori and Māori organisations. These range from hapū to Māori health providers to data sovereignty experts. This will in turn put us in the position to achieve better privacy outcomes for indigenous communities.

Māori organisations increasingly expect government agencies such as our Office to have a strong understanding and capabilities relating to the Treaty of Waitangi / Te Tiriti o Waitangi, tikanga Māori and te ao Māori. Section 21(c) of the Act requires the Privacy Commissioner to take account of these perspectives when exercising his functions, powers and duties. We recognise that to be an effective privacy regulator we need to be able to consider privacy through a te ao Māori lens.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- expand the capability and confidence of staff to engage effectively with Māori and in te ao Māori through training in te rēo Māori, tīkanga, and kawa
- prioritise empowering Māori to use their privacy rights
- provide the public sector with greater clarity about the application of the Treaty of Waitangi to privacy issues and te ao Māori perspectives on privacy and support all agencies to better understand and accommodate cultural privacy perspectives
- develop strong partnerships with and across te ao Māori and have these partnerships shape our priorities and approach to our work.

The challenges ahead of us

There are significant challenges for us to take a te ao Māori approach to privacy. We have high expectations about our understanding and capabilities relating to the Treaty, tikanga Māori and te ao Māori. These expectations emphasise the importance of putting in the work to make our engagement worthwhile to Māori.

Working alongside Māori to identify and design effective ways of building privacy awareness is a new challenge for us. Over the coming year we are starting a project to build privacy awareness with rangatahi, beginning with the development of key messages and approaches. More Information on the development of this project is in the case study for this section.

Our progress and achievements in 2025/26

During the year we continued to consult and work with Te Ranga Tautiaki, our Māori reference panel. Doing so enables us to better account for te ao Māori perspectives and make new connections when further Māori engagement is required. This panel meets quarterly and is providing advice on our work programme. The case study for this section provides an example of how Te Ranga Tautiaki brings value to our work programme.

We continued to elevate organisational cultural competency through initiatives that improved understanding, informed advice, produced better decisions and engaged Māori stakeholders. Strategic deliverables included a three-month webinar training programme, on-demand digital training resources, experiential learning about rangatahi communications, execution of our annual Māori Capability Plan, and development of te ao Māori frameworks for teams.

As a part of the Māori Capability Plan, all staff have the opportunity and are encouraged to learn te reo through an online provider. These initiatives helped develop the cultural proficiency of all staff to generate responsive, compelling and impactful privacy outcomes for Māori.

These skills were put into use this year with the Inquiry into the Manage My Health breach. Our staff needed to visit Northland because around 91 percent of those affected lived in the area, many of whom are likely to be Māori. Thanks to the support of Ngati Hine Hauora Trust, which generously hosted the event for us, we were able to hear from the right people to truly understand how the breach affected local people and impacted trust in health systems.

This year we also held the Sir Bruce Slane Memorial Lecture, in honour of New Zealand's first Privacy Commissioner. This lecture is delivered by an invited guest on a privacy law topic, and this year we were honoured to have Justice Christian Whata (Ngāti Pikiao and Ngāti Tamateatūtahi – Kawiti of Te Arawa) speak on the tapu of privacy; viewing privacy through a tikanga lens.



We continued to elevate organisational cultural competency through initiatives that improved understanding, informed advice, produced better decisions and engaged Māori stakeholders.

Assessing our impact

Indicator	Māori awareness of right to access personal information under the Privacy Act
Baseline (year)	50% (2022)[4]
Desired change	Increase
2025/26 result	**56% (2026)[5]**
2024/25 result	51% (2025)[6]
2023/24 result	54% (2024)[7]

This indicator is the closest that we have for measuring privacy outcomes for Māori. The right to access personal information under the Act is important and awareness of that right is a useful proxy for general privacy understanding. Our ambition is to increase the level of awareness over time.

We measure this indicator through our annual privacy survey, which surveys more than 300 Māori adults each time it is conducted. With our baseline result of 50% in 2022, our subsequent surveys are showing a small increase in awareness of the right to access personal information, with the 2026 result being 56%. We consider this result to be a positive sign of achieving our outcomes.

Indicator	All externally reviewed policy files appropriately incorporate Treaty and te ao Māori analysis as necessary
Baseline (year)	New measure
Desired change	Maintain
2025/26 result	**See Statement of Service Performance Function 4 for further details on achievement or result.**
2024/25 result	Achieved
2023/24 result	Achieved

Every year our policy work is independently audited as a quality assurance check using the government Policy Quality Framework. One aspect of this review is whether our policy work appropriately incorporates Treaty and te ao Māori analysis.

The external review for 2025/26 again identified that, although there was limited consideration of te ao Māori perspectives, where it was covered, it was done well. We are satisfied with this result as it maintains what we achieved in 2024/25.

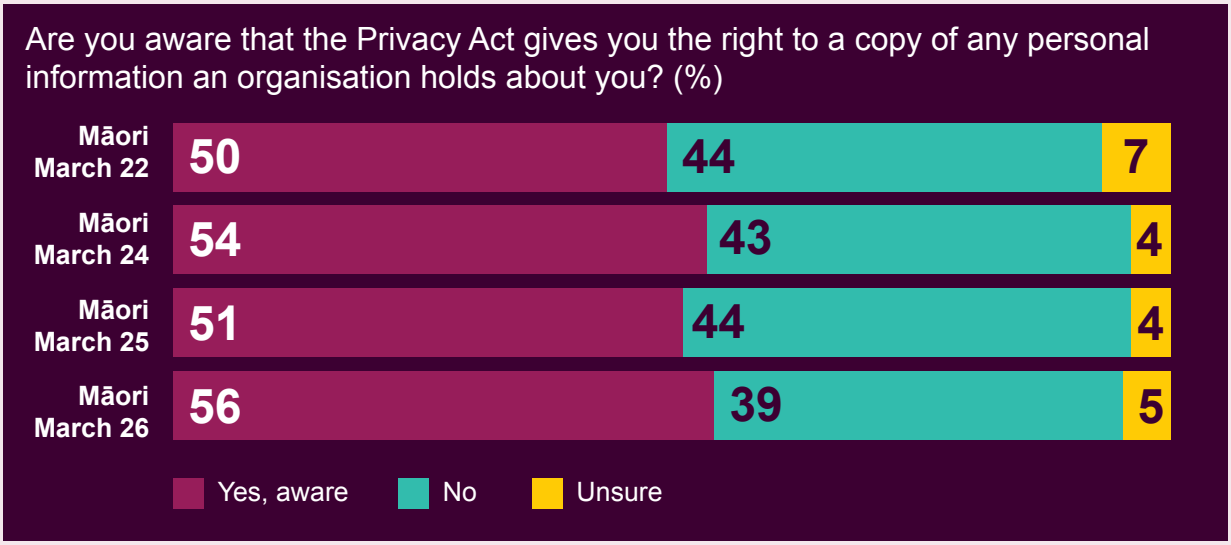
Indicator	Continued implementation of our Mahere Reo strategy and training to develop staff understanding of te ao Māori
Baseline (year)	New measure
Desired change	Increase
2025/26 result	**Achieved**
2024/25 result	Achieved
2023/24 result	Achieved

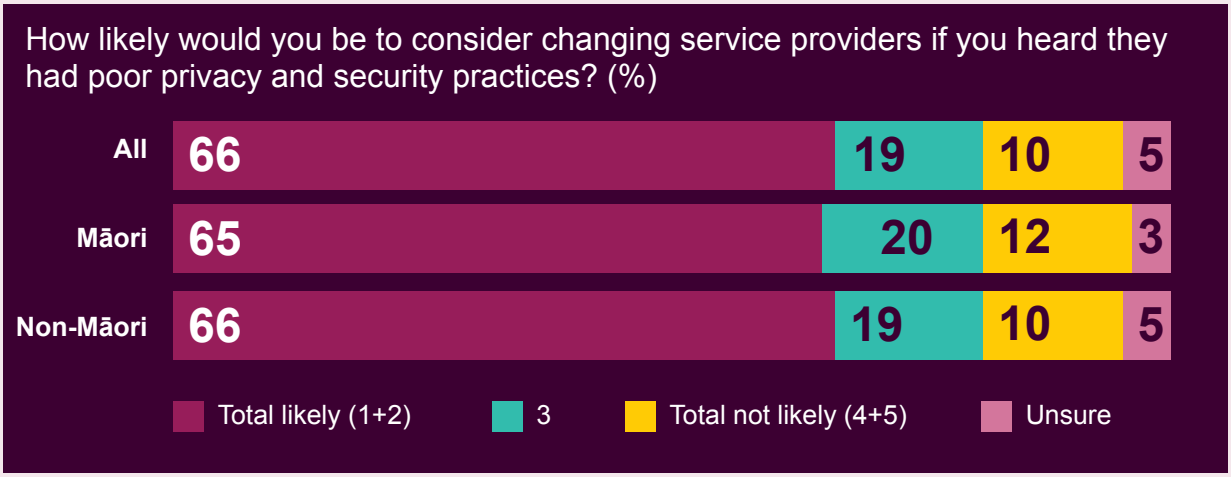
Our Mahere Reo (Māori Language Plan) supports the Māori Language Act 2016 and the Maihi Karauna. To that end, it targets an environment that fosters te reo Māori to enhance services to Māori stakeholders, grow a confident and capable workforce, and comply with our statutory requirement to take account of cultural perspectives in privacy.

Our accomplishments in 2025–2026 included making te reo more visible in our public sector planning and reporting documentation and recruitment materials, offering te reo courses for all staff, and expanding the use of te reo Māori greetings in staff communications.

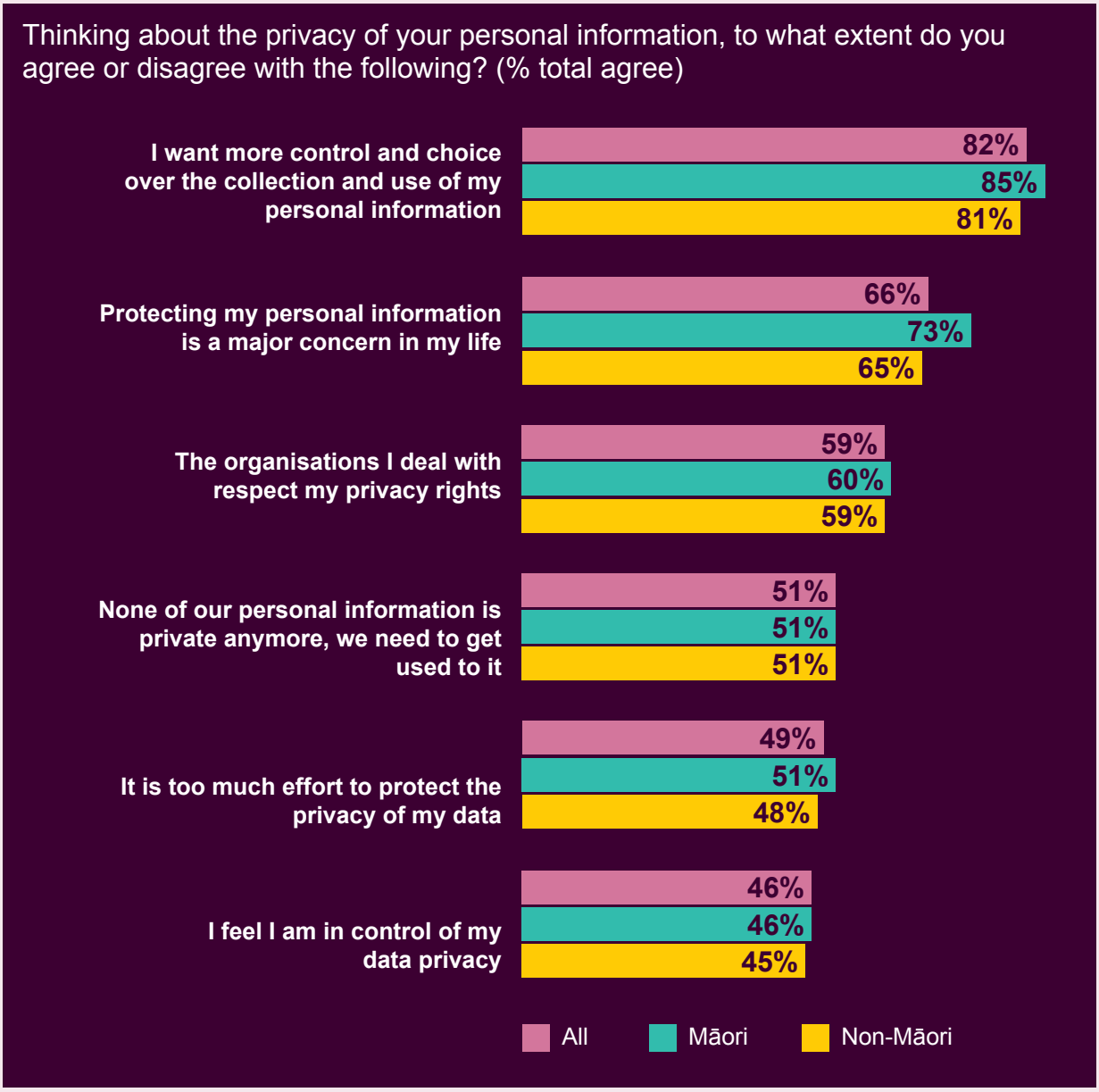
4. *Privacy concerns and sharing data, Omnibus research commissioned by the Privacy Commissioner*. AK Research & Consulting March 2022.
5. *Research on Privacy Concerns and Use of Personal Information*, AK Research and Consulting April 2026
6. *Research on Privacy Concerns and Data Sharing*, AK Research & Consulting March 2025.
7. *Research on Privacy Concerns and Data Sharing*, AK Research & Consulting April 2024.

Māori experiences related to privacy





Source: Research on Privacy Concerns and Use of Personal Information, AK Research and Consulting April 2026


Thinking about the privacy of your personal information, to what extent do you agree or disagree with the following? (% total agree)
I want more control and choice over the collection and use of my personal information
82%
85%
81%
Protecting my personal information is a major concern in my life
66%
73%
65%
The organisations I deal with respect my privacy rights
59%
60%
59%
None of our personal information is private anymore, we need to get used to it
51%
51%
51%
It is too much effort to protect the privacy of my data
49%
51%
48%
I feel I am in control of my data privacy
46%
46%
45%
All
Māori
Non-Māori

1

CASE STUDY

Developing Rangatahi Kōkiri – engaging with young Māori

Te Ranga Tautiaki, our Māori Reference Panel, proposed that we develop a project to promote the understanding on privacy rights with rangatahi Māori. We have taken up this wero as children and young people can be more at risk of privacy (and other) harms, and the Act requires that we take account of cultural perspectives on privacy. Promoting the understanding of privacy rights with rangatahi will help them develop habits and behaviours that may affect how they manage privacy throughout their lives.

Te Ranga Tautiaki have assisted us with finding a partner to co-design a pilot project, which will be developed during the 2026/27 year. This pilot will develop key content, messages and approaches alongside rangatahi to build privacy awareness. This collaborative approach will be one way that we take account of te ao Māori perspectives during the project.

We have named our project Rangatahi Kōkiri, and it will build our experience in engaging with rangatahi on privacy issues. This name emphasises the essential role of rangatahi to champion, promote, advocate and lead initiatives that are for and about them – including this campaign to raise rangatahi awareness about their rights to privacy.



Objective 2:
We will engage and empower people and communities who are more vulnerable to serious privacy harm

Our functions that directly support Objective 2: Communication and Education.

The Act provides New Zealanders with important rights they can use to increase their confidence that their privacy is being protected and to protect themselves from privacy harm. These rights include being informed about why an agency is wanting to collect their personal information and who will receive the information. After collection, the Act then provides New Zealanders with a right to access a copy of their information and to seek a correction should the personal information be incorrect.

Through exercising their privacy rights, individuals have an important role in ensuring privacy is a core focus for agencies. Agencies will prioritise privacy if their customers and clients challenge them on why and how much personal information is being collected, seek corrections to their personal information or complain if their privacy has been interfered with. New Zealanders are also proactive about letting us know about areas of non-compliance or privacy concerns that they have.

Focusing on outreach and engagement helps us promote an understanding of privacy rights. Our aim is to connect with people and communities who are more vulnerable to serious privacy harm to ensure we can help improve their privacy outcomes. We do this through our contemporary and regularly updated website, AskUs knowledge database, a monthly newsletter, free brochures being available in multiple languages and formats, LinkedIn, regular events and presentations, and our media related activities.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- improve our digital service channels so that they provide people with what they need (including replacing our existing website)
- undertake outreach and engagement activities focused on understanding those parts of society that are more vulnerable to serious privacy harm and working with others to empower them to use their privacy rights.

The challenges ahead of us

New Zealanders are living in an increasingly complex environment when it comes to their privacy rights. For example, new technologies keep appearing, often with detailed terms of service documents. This environment emphasises the need for New Zealanders to be aware of their privacy rights but also leads to notification fatigue, clicking ‘Accept’ without engaging, and a feeling of their personal information being out of their control.

Some people and communities in New Zealand are more vulnerable to serious privacy harm. This includes children, elderly, the disabled community, the rainbow community, Māori and immigrant communities. It can also include people in vulnerable situations, like children in the Oranga Tamariki system, beneficiaries, victims of crime, inmates, and patients in the health system.

The challenge for our Office is to be adaptable in how we connect with New Zealanders so that they can better understand their privacy rights.

Our progress and achievements in 2025/26

This year our key achievements for engaging people and communities included:

- Completing our in-house website redevelopment to simplify the website structure, shift it into a plain language framework, increase accessibility, and make the majority of content web content.
- Simplifying and improving the 650 popular privacy questions in our AskUs knowledge base, and creating a suggestion form so people can tell us about new content they want to see.
- Significantly improving the accessibility of our material through ensuring our privacy rights information is available in Easy Read, sign language, Braille, and in six new languages.
- Releasing a range of guidance targeted at improving the privacy outcomes of children and young persons, as outlined in the case study of this section.
- Receiving 133 requests for speeches and presentations across the motu, which saw various staff speaking to groups serving vulnerable communities such as health providers, churches, schools, English language schools, and not for profit groups.
- Receiving and responded to 176 media enquiries.

The above achievements have supported us in shifting how we handle public enquiries this year. For many years we operated a bespoke enquiries service where we provide customised answers for several thousand people and agencies who would email or call us with their privacy questions. For example, this year we responded to a total of 5,093 enquiries between 1 July 2025 to 30 April 2026.

Following an independent review, this year we changed how we provide our public enquiries service for individuals and agencies that contact us. We moved away from a bespoke public enquiries service and towards a one-to-many self-help service utilising our existing website and AskUs knowledge base. The changes to our enquiries functions mean that the data in the next section shows a large drop in enquiries volumes in the final quarter of the 2025/26 year, reflecting the closure of our call centre and enquiries email address.

Assessing our impact

Indicator	Public awareness of right to access personal information under the Privacy Act
Baseline (year)	47% (2022)[8]
Desired change	Increase
2025/26 result	**55% (2026)**
2024/25 result	53% (2025)
2023/24 result	50% (2024)

The public's awareness of their privacy right to access personal information is an important indicator for the outcome that 'individuals are more confident that their privacy is protected'.

We use this indicator as a proxy for privacy understanding of individuals and measure it through our annual privacy survey. The right to access personal information is a long standing right and was in the Privacy Act 1993. Exercising your right to access personal information then allows you to exercise another of your privacy rights: your right to request that an agency correct your personal information.

Our 2022 baseline result of 47% awareness of the access right was a mixed result as it left significant room for improvement.

8. Privacy concerns and sharing data, Omnibus research commissioned by the Privacy Commissioner. AK Research & Consulting March 2022.

The privacy surveys we undertake are showing small but consistent increases in the awareness of the right to access personal information. This is very encouraging – we believe that New Zealanders who understand their privacy rights are more likely to be able to protect themselves from privacy harms.

Indicator	Significant improvements made to digital service channels
Baseline (year)	New measure
Desired change	Increase
2025/26 result	**Achieved** See Statement of Service Performance Function 2 for further details on achievement or result.
2024/25 result	Achieved
2023/24 result	Achieved

The improvements made to our digital service channels over recent years have enabled the shift to the one-to-many self-help service this year. As noted above, improvements to our digital service channels included completing our website redevelopment process and reviewing the AskUs knowledge base.

Indicator	Respond to all public enquiries within five working days
Baseline (year)	99% (2021/22)[9]
Desired change	Maintain
2025/26 result	**68%**
2024/25 result	90%
2023/24 result	96%

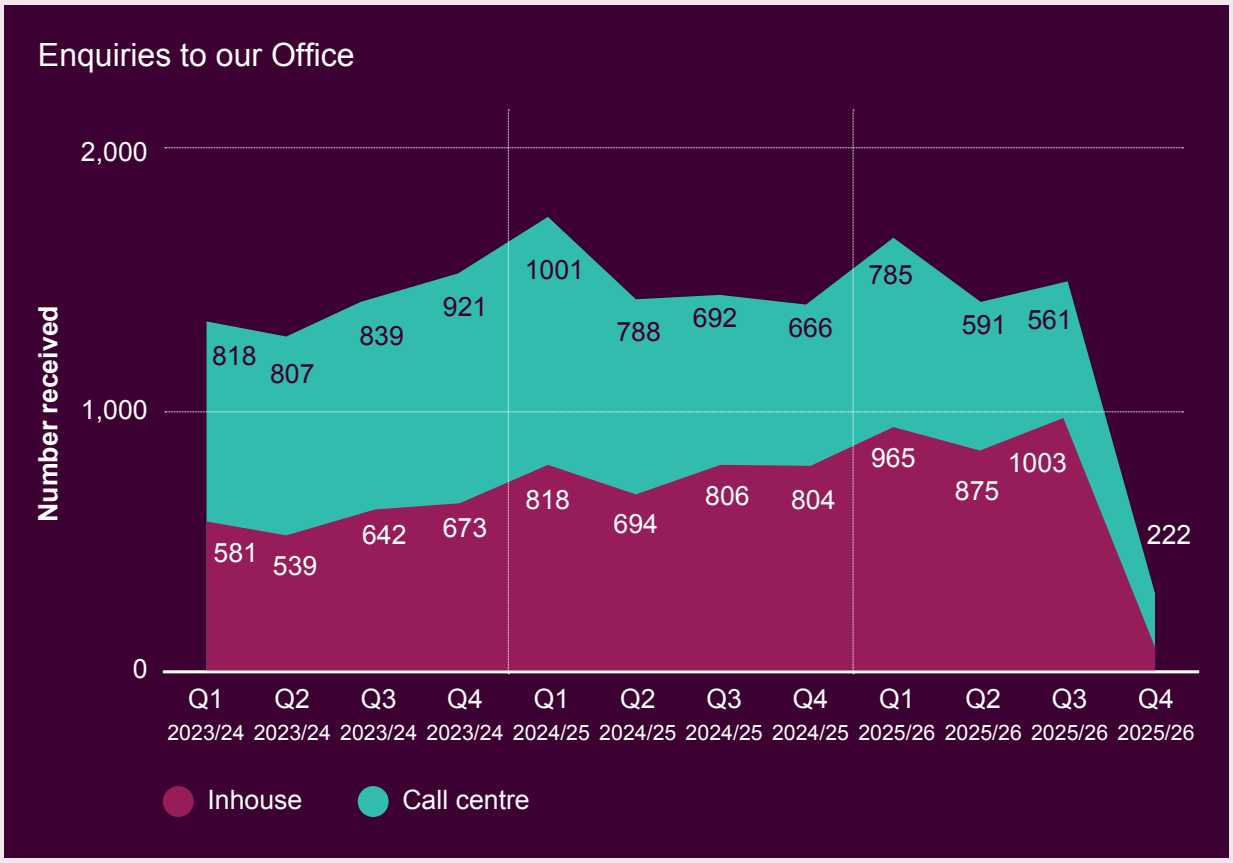
We seek to promptly respond to public enquiries because informed individuals can better exercise their privacy rights and protect themselves. Our baseline results for this indicator was excellent, with 99% public enquiries responded to within five working days in 2021/22 and 2022/23.

The timeliness of our responses to public enquiries decreased as the pressure on our teams increased while our resources remained at the same level. During the 2025/26 year it become evident that the volume of public enquiries that we were responding to within five working days was dropping significantly. The drop in timeliness was one of the reasons we commissioned the independent review outlined above.

9. The figure reported in the 2022 Annual Report of 94% was against a measure of responding within 2 working days. The figure shown here has been calculated at 5 working days for comparative purposes.

Data relating to our enquiries functions

Note that the figures for quarter 4 of 2025/26 are very low due to the changes to our enquiries function made during that quarter.



2

CASE STUDY

Guidance to help protect the privacy and safety of children and young people

Children and young people in New Zealand have the same privacy rights as adults and can expect that their personal information is protected. However, they are more vulnerable to privacy harms and require additional care to ensure that their privacy is protected. Improving how a child or young person's personal information is respected and protected will help reduce privacy harms that can arise.

During this year we released a range of guidance to help agencies better protect the privacy of children.

Guidance for the education sector

This extensive guidance was designed to help frontline workers in the education sector make sure personal information is properly used and protected. It uses a range of real-world situations to help people working in education make good privacy decisions with confidence.

This guidance provides information on how educational agencies can

- collect, use, and share the personal information of children and young people.
- retain and dispose of personal information.
- manage information requests, privacy complaints and privacy incidents.

Guidance for multi-agency information sharing meetings

This set of guidance is targeted at meetings where multiple agencies are working together to improve outcomes for children and young people. This includes situations such as Police-led multi-agency meetings to reengage youth offenders in education or employment. The objective of the guidance is to help promote greater information sharing in an authorised and protective manner. A template information sharing protocol is provided for use by agencies.

Guidance related to child safety concerns

The Privacy Commissioner has also been very clear about his expectation that personal information should be shared where there are concerns about the safety of a child. He made these comments in October 2025 when the Government responded to Dame Karen Poutasi's independent review of the children's system. The Commissioner also spoke to regional public service leaders to ensure they were confident in how information sharing can protect the wellbeing and safety of children and young people.

Supporting these statements, we released guidance on information sharing (whether under the Privacy Act, Oranga Tamariki Act 1989 or Family Violence Act 2018) and launched www.whatcanishare.org.nz as an easy way to access our guidance.

Objective 3:
We will set clear expectations to provide agencies with greater certainty about their responsibilities

Our functions that directly support Objective 3: Policy and Advocacy.

Our Office needs to set clear expectations so that agencies can better understand what the Act requires of them. We achieve this by issuing guidance, maintaining up to date codes of practice (secondary legislation), and having free tools for agencies to use (such as our e-learning modules).

The requirements under the Act involve agencies collecting, using and sharing personal information in a privacy protective manner. This includes notifying individuals about what personal information the agency is collecting, storing personal information securely, and only using or disclosing the personal information for specific reasons.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- provide agencies with greater certainty through setting specific, strong, and clear expectations, focusing on areas where there are the most significant power imbalances between individuals and agencies and/or sensitive information is involved
- support agency understanding and capability by supporting the development of, and engaging with, the privacy profession (both in-house privacy professionals and privacy advisors)
- ensure that codes of practice issued under the Act and our guidance, advice and education material are fit for purpose
- expect Government and businesses to demonstrate that their privacy related activities are necessary and proportional.

The challenges ahead of us

The Act takes an adaptable, principles-based, approach to regulation and is best viewed as a ‘how to’ (rather than a ‘do not do’). This means that managing privacy well is not a tick box exercise – agencies must understand what to do in their specific circumstances. The Act also applies to nearly the entire public, private and not-for-profit sectors. There are also new technologies that create new and novel situations to consider privacy within. Agencies must understand what to do in their specific circumstances, although we can issue and review codes of practice under the Act that amend requirements for different sectors or types of personal information.

These factors lead to a large demand for certainty from us as the regulator. This is why we focus on producing excellent guidance for agencies and privacy advice on the government’s legislative programme.

Our progress and achievements in 2025/26

Providing clear guidance to agencies has continued to be a major focus for our Office. Our guidance is in plain language, highly engaged with and is a practical, supportive way to help agencies do privacy well. We are proud of our achievements in this area.

The creation of the Biometric Processing Privacy Code in August 2025 was a major event for our Office, and the culmination of several years of effort. This Code sets more specific rules for agencies using biometric technologies to collect personal information, and is supported by comprehensive guidance. The Code provides greater clarity and certainty to agencies and we have received feedback that agencies appreciated the constructive and pragmatic approach we have taken to this increasingly widespread technology. Our work on biometrics has continued, and we are developing additional guidance in specific areas before shifting to a compliance-led approach.

In October 2025 we amended the Telecommunications Information Privacy Code 2020 to better support search and rescue operations and to ensure this Code would work as intended. Schedule 4 of this Code was amended in 2020 to allow emergency services to locate 111 callers and mobile phones in certain emergency situations, while maintaining privacy safeguards. Operational changes since 2020 meant that the Code required an update to ensure that emergency services could continue to function.

In February 2026, we joined 60 other privacy and data protection authorities in issuing a Joint Statement on AI Generated Imagery. This Joint Statement was issued in response to serious concerns about AI systems generating realistic images and videos depicting identifiable individuals without their knowledge and consent. Agencies were reminded that AI content generation systems must be developed and used in accordance with privacy legislation and we outlined four principles that agencies should follow when developing and using such systems.

A privacy highlight of the year was the creation of a new privacy principle in the Act. On 1 May 2026, the Privacy Amendment Act established a new indirect notification requirement for agencies: Information Privacy Principle 3A. We put in a lot of effort to support the introduction of this new principle, including comprehensive guidance, creating a video, and delivering a range of in-person presentations and webinars. More information on this work is available in the case study for this section.

Every year in May we run ‘Privacy Week’, and our 2026 theme was ‘Foundations of the Future’. We had 18 free webinars watched by over 5,500 people during the week. The most popular topics included 'Privacy after search. What changes when AI becomes the interface to organisational knowledge?’, ‘On Privacy and Technology’ and ‘In the Eye of the Storm: Navigating Privacy Incidents with Clarity and Control’.

We also provide government agencies, Cabinet and Parliament advice on the privacy implications of the Government’s legislative programme. A key aspect of our advice is to consider whether proposed legislative amendments are necessary and that the impacts on personal privacy are justified and proportionate. Over the year we provided privacy advice to dozens of agencies and made a total of 14 submissions to Parliamentary Select Committees.

A significant select committee submission that we made this year was on the Policing Amendment Bill. One part of this Bill authorises the New Zealand Police to record images and sounds in public and private places and to collect personal information for lawful purposes, including intelligence.[10] We did not support these aspects of the Bill and recommended they were not proceeded with, or at the least proceeded only with additional safeguards. While the Justice Select Committee did not recommend halting the Bill as we recommended, it did recommend some changes to the Bill to address some of our concerns. These changes include clarifying the relationship between the Bill and the Privacy Act and requiring a statutory review after 3 years.

During the year we also made legal submissions in a Court of Appeal case considering the lawfulness of New Zealand Police using automatic number plate recognition on the Auror software platform. Our submissions to the Court as an intervener focused on the privacy implications of this technology and application of the information privacy principles of the Act, in the context of a large commercial platform (Auror) automating the delivery of number plate and associated information from retailers to Police.

Assessing our impact

Indicator	Awareness of Privacy Act requirements
Baseline (year)	New measure
Desired change	Increase
2025/26 result	**See next subsection**
2024/25 result	See Annual Report 2024/25
2023/24 result	See Annual Report 2023/24

The broad scope of the privacy system makes it difficult to gauge the level of awareness that agencies have of the Act's requirements. Many agencies have a low level of understanding of the Act and those that we do interact with are often not aware of their full obligations under the Act.

To estimate the awareness of requirements under the Act, in recent years we have leveraged the results of surveys undertaken by other agencies – such as the Institute of Directors. We took this approach as our limited resources mean that we cannot engage with a representative sample of agencies in New Zealand to build a comprehensive picture of privacy understanding across the economy.

This year we took a different approach, by sending a short anonymous survey to agencies who reported a privacy breach or incident to us. High-level results of this survey are available in the next section.

Indicator	Undertake two projects per year relevant to setting privacy standards, expectations, or guidance in the privacy system
Baseline (year)	New measure
Desired change	Maintain
2025/26 result	**Achieved** See Statement of Service Performance Function 4 for further details on achievement or result.
2024/25 result	Achieved
2023/24 result	Achieved

This indicator is an important part of ensuring that we continue to set clear expectations for agencies in the privacy system. Significant projects related to setting privacy standards, expectations or guidance this year were:

- amending the Telecommunications Information Privacy Code 2020 to better support the sharing of location information
- supporting the new indirect notification principle in the Act with guidance, privacy code amendments, and sector specific guidance.

10. Note that this Bill arose in part due to the 'Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public' that was completed in September 2022. The Bill also responded to a Supreme Court decision in a case (Tamiefuna) in which the Privacy Commissioner had made privacy submissions.

Indicator	Percentage of externally reviewed policy files that are rated as 3.5 out of 5 or better for quality
Baseline (year)	95% (2022)
Desired change	Maintain
2025/26 result	**93%** See Statement of Service Performance Function 4 for further details on achievement or result.
2024/25 result	93%
2023/24 result	100%

Ensuring that we undertake high-quality work is an important aspect of ensuring that the work we are doing is likely to set clear expectations for agencies. This annual review is undertaken by an external evaluator and assesses a random sample of the work undertaken by our Policy team. We have continued to receive a strong result in this area.

Data relating to agency privacy understanding

Insights from agencies that notified breaches to OPC in 2025/26

This year we sent a short anonymous survey to the 668 agencies who had notified our Office of a privacy breach or incident over the preceding 12 months. Agencies that had notified us of multiple breaches or incidents received a single survey link.

This was the first survey of its type that we had undertaken. Our aim was to better understand the processes that agencies undertake when a privacy breach or incident occurs and their level of privacy understanding and capability.

The questions we asked in the survey were derived from our guidance on how agencies can do privacy well: Poupou Matatapu.

A total of 217 agencies completed the survey, with 58 responses from the public sector, 118 from the private sector and 41 from the not-for-profit sector.

High-level results from the responding agencies included:

- 77% used our Notify Us self-assessment form before submitting their privacy breach or incident to our Office.
- 76% had their own process for assessing whether a privacy incident reached the threshold for notifying our Office.
- 90% undertook a lessons learned debrief after notifying our Office of the breach or incident.
- 91% have a Privacy Officer.
- 79% regularly brief their organisation's senior leadership or board of directors about privacy issues.
- 50% conduct regular audits to ensure personal information is being accessed only as intended.
- 78% consider what privacy training specific roles within their agency should receive.
- 81% have a response plan prepared in case of a privacy breach.

This data is interesting but subject to limitations. For example, we could only survey those agencies that had contacted us about a privacy breach or incident, and so the data may not be representative of the privacy system as a whole.

3

CASE STUDY

Guidance for the new Information Privacy Principle 3A on indirectly collecting personal information

On 1 May 2026, the new Information Privacy Principle 3A came into force, changing the obligations that agencies have when they collect personal information about an individual indirectly (from someone other than the individual themselves). The new principle requires that an agency collecting someone's personal information indirectly is required to notify the individual unless an exception applies.

We published comprehensive guidance to support agencies in understanding and implementing this new privacy principle. This guidance explained what the new principle covered and how we consider that agencies can meet key requirements, such as when individuals should be notified about their personal information being collected. A variety of examples and a decision flowchart were provided to assist agencies.

The guidance we provided to agencies extended beyond information on our website. We created a short video and webinars to help agencies understand their new obligations and presented in-person to a variety of forums and industry body groups.

We also amended codes of practice issued under the Act to incorporate the new principle 3A where appropriate. These Codes modify the information privacy principles for specific sectors (such as the health sector) and technologies (such as biometric technologies). By incorporating principle 3A into these codes we reduce uncertainty for agencies. We then supported amendments to the Health Information Privacy Code with specific guidance for the health sector about rule 3A.

We received significant positive feedback from agencies about our work in this area.





Objective 4:
We will promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm

Our functions that directly support Objective 4: Compliance and Enforcement, Investigations and Dispute Resolution.

We encourage and support agencies in meeting their privacy requirements. We also act to hold agencies to account where necessary to address non-compliance. Our Compliance and Regulatory Action Framework sets out our escalation approach to encourage agencies to meet their requirements.

Using our full range of investigation and compliance powers promotes stronger privacy outcomes. For example, we issue compliance letters setting out our expectations with agencies about their privacy practices, issue compliance notices requiring agencies to alter their practices and publicly name agencies we find to be in breach of the Act in line with our Naming Policy. The use of these tools ensures the sector understands how we will respond when needed.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- have our compliance activities prioritise systemic privacy issues relating to those parts of society that are more vulnerable to serious privacy harm, especially when those issues stop individuals from exercising their privacy rights
- promptly triage and investigate privacy complaints and breach notifications, while accounting for cultural needs and recommending redress where possible
- inform our work with insights from identified privacy system risks, international experiences and our own data.

The challenges ahead of us

We are receiving high volumes of privacy breaches notifications and complaints. Individual breaches can be very complex, and like many similar agencies we are encountering increasing numbers of abusive individuals. These factors place increasing pressure on our staff and the accomplishment of our key performance indicators.

The demands on our functions mean that we constantly prioritise the use of our investigation and compliance powers. This demand arises from the broad scope of the privacy system, where privacy breaches and complaints can occur anywhere and be very different in cause, impact, sector and size.

The lack of penalties within the Act provides agencies with few financial incentives to take privacy seriously. This situation means that we encounter many agencies that have a low level of understanding of the Act.

Our progress and achievements in 2025/26

During 2025/26 our Investigations and Dispute Resolution function again experienced extremely high levels of privacy complaints, with 1,644 privacy complaints received from individuals. We took a 'fast resolve' approach to 1,236 of these complaints, for example by encouraging the person to first approach the relevant agency with their complaint. This approach promotes the best outcomes for complainants within a quick timeframe.

One privacy complaint that was closed this year was a representative complaint involving more than 1,600 affected individuals. Note that for the purposes of the complaint volume data in the next section, this is done on a per file basis and so this representative complaint is treated as a single privacy complaint (in line with prior years).

Where we investigate a privacy complaint, we have a strong dispute resolution mandate and negotiated financial settlements for 3.1% of the privacy complaints. Investigating and resolving privacy complaints is very important to complainants because it provides them with redress and helps restore their confidence that their privacy is protected.

For privacy breaches notified to us by agencies, the 2026 year began with two cybersecurity breaches in the health sector: the Manage My Health patient portal, and the MediMap medication management platform. These were breaches of platforms used by hundreds of health sector agencies and had a widespread, but variable, impact.

We launched an Inquiry into the Manage My Health breach in January. Phase one of the Inquiry was completed in May 2026 and found that Manage My Health and Health New Zealand had failed in their responsibilities to have reasonable security safeguards in place. Phase two of the Inquiry is ongoing.

This year our compliance function received a total of 2,231 privacy breach notifications. This dramatic increase (the 2024/25 figure was 1,093) was caused by the large number of agencies related to the Manage My Health and MediMap breaches. All of these privacy breaches need to be assessed, reviewed and then followed up where they are likely to cause serious harm. Our activities in this area encourage agencies to swiftly address privacy breaches and to build their capability to help avoid future privacy breaches.

Our compliance activities also involve working with agencies to improve their privacy practices. A significant example of this work during the year was working proactively with NZ Transport Agency Waka Kotahi on a privacy uplift programme they have initiated in response to several serious harm privacy breaches of the Motor Vehicle Register. This programme will deliver significant changes to the regulatory approach to safeguarding personal information held on both the Motor Vehicle and Driver Licence Registers.

Assessing our impact

Indicator	Percentage of serious privacy breaches notified to our Office within 72 hours
Baseline (year)	61% (2022/23)
Desired change	Increase
2025/26 result	**86%**
2024/25 result	71%
2023/24 result	60%

We assess our impact in this area though the promptness for which serious privacy breaches are notified to our Office. It is a statutory requirement for agencies to notify the Privacy Commissioner as soon as practicable of any privacy breach where it is reasonable to believe an individual could suffer serious harm. We have issued clear guidance that we expect these notifications to be provided to us within 72 hours.

In 2023/24 we had 60% of serious privacy breaches notified to our Office within 72 hours and we are aiming to improve this percentage. The 2024/25 percentage increased to 71%, in part due to a series of similar breaches being notified promptly by one particular sector.

The increase to 86% for 2025/26 reflects the impact of the Manage My Health and MediMap breaches. The high number of agencies that reported these breaches to us mean that they have an outsized impact on this statistic this year. Both MediMap and Manage My Health notified our Office within the 72 hours of being made aware of their respective breaches.

Indicator	**Notified privacy breaches that are likely to cause serious harm, are followed up with the notifying agency within 10 working days of risk assessment**
Baseline (year)	New measure
Desired change	Maintain
2025/26 result	**99.8%** See Statement of Service Performance Function 3 for further details on achievement or result.
2024/25 result	95%
2023/24 result	85%

We follow up with agencies who have notified us of serious privacy breaches to help ensure that agencies are responding well and mitigating the harm to affected individuals. Our target for this measure in 2023/24 was a 100% follow up rate.

The result for 2025/26 is 99.8%. This high percentage this year is again impacted by the Manage My Health and MediMap breaches, as both were followed up with within 10 working days.

Indicator	**The percentage of complaints closed during the year that were less than six months old at closure**
Baseline (year)	84% (2022/23)
Desired change	Maintain
2025/26 result	**40%** See Statement of Service Performance Function 5 for further details on achievement or result.
2024/25 result	88%
2023/24 result	75%

We are seeking to maintain timeliness in resolving privacy complaints so that agencies know we act promptly when serious privacy harms occur. For this measure we also include our ‘fast resolve’ complaints.

The 2024/25 result of 88% reflected a good result during a period of high and increasing volumes. However, we were mindful that high volumes and limited resourcing increased the wait time for an investigator to be available.

The 2025/26 result is 40% and is driven by a complaint file closing in April 2026 that was first received in November 2024. This was a representative complaint file constituting 1,672 individual complaints, which consequently has an outsized impact on this particular measure (as this single complaint file involves a large number of complaints). If the complaints in this file are excluded from the figures, the percentage of complaints closed during the year that were less than 6 months old at closure sits at 85%.

Indicator	The percentage of externally reviewed compliance investigations that are rated as 3.5 out of 5 or better for quality
Baseline (year)	New measure
Desired change	Maintain
2025/26 result	**100%** See Statement of Service Performance Function 3 for further details on achievement or result.
2024/25 result	100%
2023/24 result	100%

We want our Compliance and Enforcement investigations to be of high quality to ensure that our interventions are correct and effective. The result of our external quality review of our compliance investigations and compliance notices continues to be extremely pleasing and we will be seeking to maintain this quality going forward.

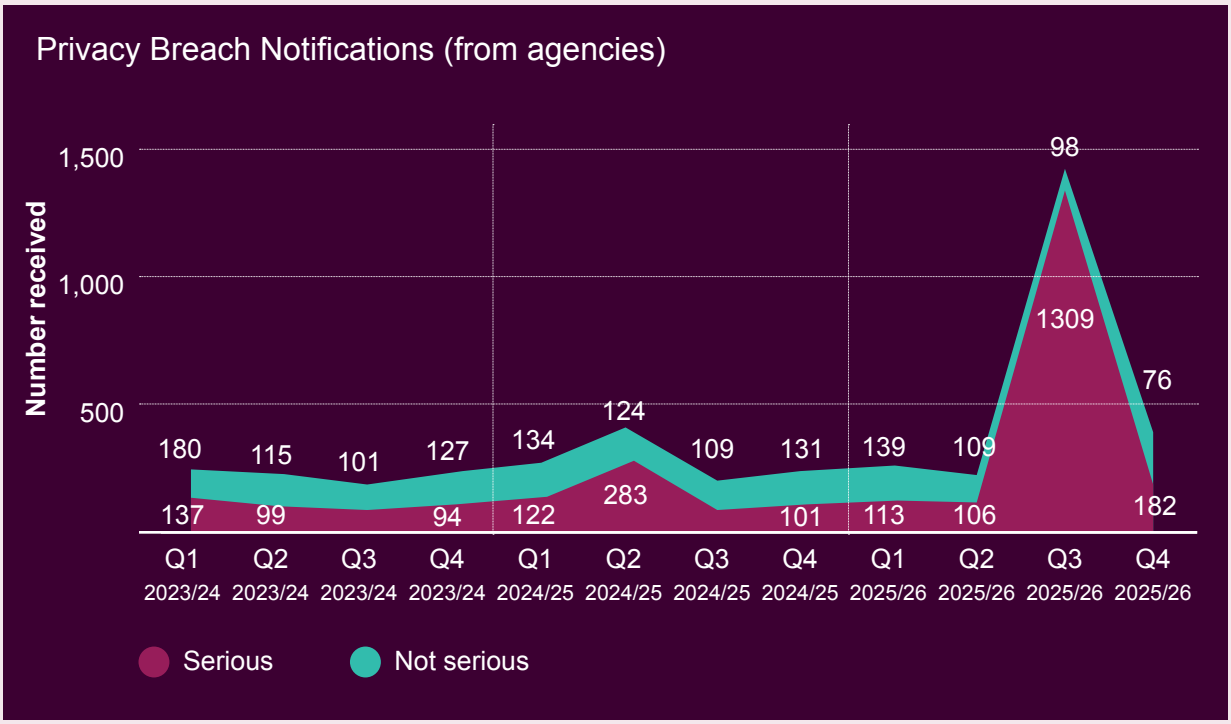
Data relating to our compliance activities

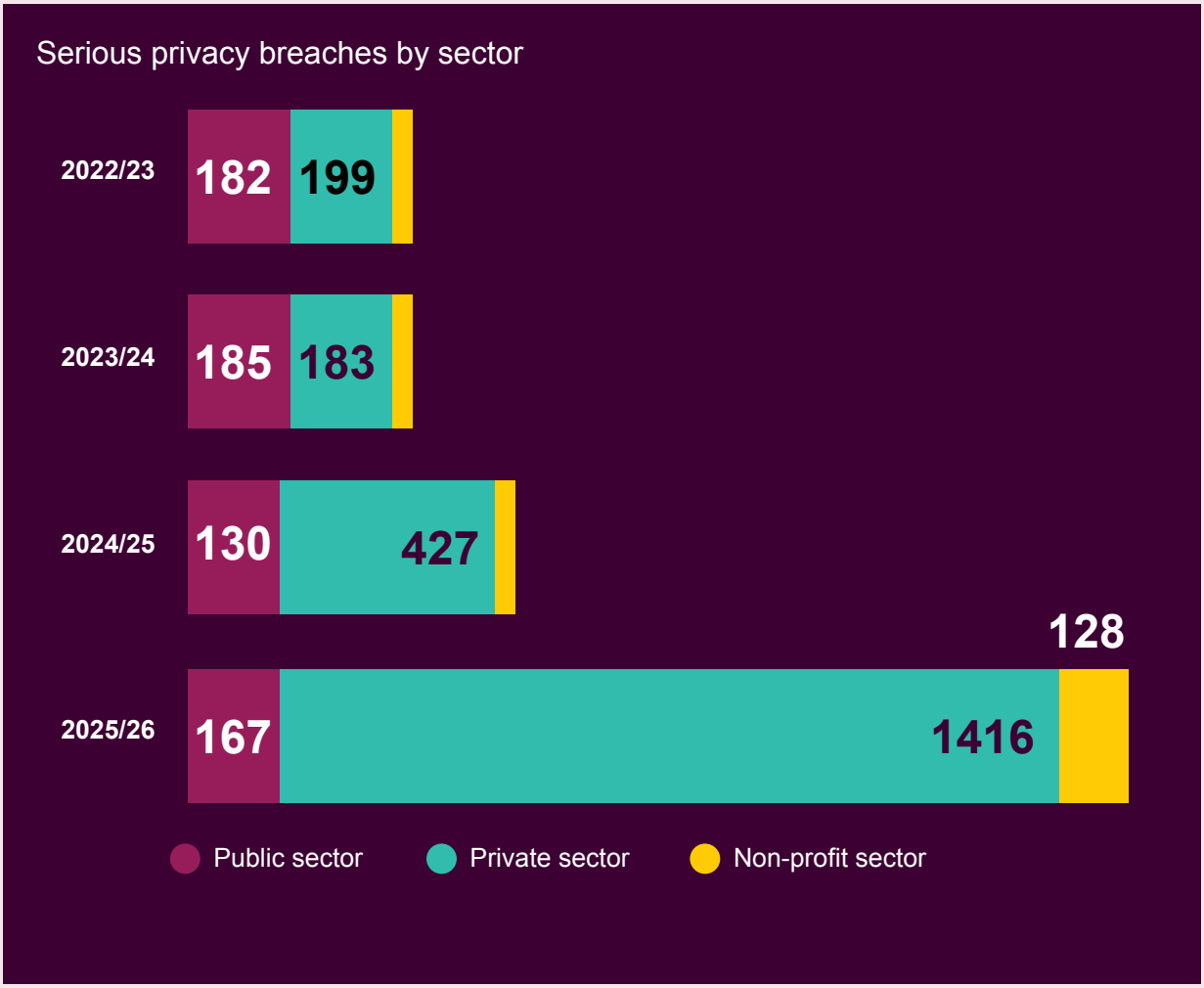


Number of complainants in a single representative complaint closed in 2025/26: **1,672**

Top complaints by agency	
New Zealand Police	98
Department of Corrections	22
Ministry of Social Development	15
Ministry of Business, Innovation, and Employment	13
Oranga Tamariki	12

Top breach notifications (serious harm only) by agency	
Te Whatu Ora – Health New Zealand	23
Department of Corrections	19
Ministry of Social Development	19
New Zealand Police	14
New Zealand Transport Agency	8


Privacy Breach Notifications (from agencies)
Number received
1,500
1,000
500
180
115
101
127
134
124
109
131
139
109
98
1309
76
137
99
94
122
283
101
113
106
182
Q1 2023/24
Q2 2023/24
Q3 2023/24
Q4 2023/24
Q1 2024/25
Q2 2024/25
Q3 2024/25
Q4 2024/25
Q1 2025/26
Q2 2025/26
Q3 2025/26
Q4 2025/26
Serious
Not serious


Serious privacy breaches by sector
2022/23
182
199
2023/24
185
183
2024/25
130
427
2025/26
167
1416
128
Public sector
Private sector
Non-profit sector

4

CASE STUDY

Addressing the anxiety and costs of a letter sent to the wrong person

We received a privacy complaint from a patient of a health agency. They were in significant distress as the health agency had mistakenly sent a letter containing their contact information to the wrong person. This mistake only became apparent when the letter recipient contacted the patient, who immediately had significant safety concerns due to who had received the letter.

The health agency acknowledged the situation and apologised but declined to provide financial compensation for the privacy breach. Once aware of breach, the health agency notified our Office of the privacy breach.

When the patient made a privacy complaint to our Office, the efforts of the patient and health agency allowed us to attempt to resolve the complaint without a full investigation.

We approached the patient and health agency to participate in a conciliation process to try and resolve the complaint. This conference allowed the patient to explain the security precautions they were now required to take and the associated costs. For their part, the health agency was able to apologise in person and explain the process improvements they had made to avoid similar problems in the future. The issue of financial redress arose and, after negotiation, a payment was agreed to meet some of the costs of the increased security protections.

Small privacy mistakes can cause significant harm. In this situation, a letter to the wrong person raised legitimate safety concerns and emotional distress that could only be addressed through the assistance of our Office.



Office and functions

Te Tari me āna mahi

Independence and other interests

The Privacy Commissioner has wide ranging functions. The Commissioner must have regard to the information privacy principles in the Act and the privacy interests of individuals alongside other important human rights and social interests.

Relevant rights and social interests include the desirability of a free flow of information and government and business being able 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 Commissioner must also take account of cultural perspectives on privacy.

The Privacy Commissioner is independent of the Executive branch of the government. 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 sharing programmes.



Relevant rights and social interests include the desirability of a free flow of information and government and business being able to achieve their objectives in an efficient way.

Reporting

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

Staff

We employ staff in our Auckland and Wellington offices. During the year to 30 June 2026, the senior leadership team was made up as follows:

- The Deputy Privacy Commissioner: responsible for 4 teams – Investigations and Dispute Resolution, Compliance and Enforcement, Capability and Guidance and Policy.
- The General Manager: responsible for Support Services and Finance and Performance, Strategy Insights and International, Communications and Engagement and our Pou Ārahi. 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

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.

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 2026	Actual 2025
$100,000 – $109,999	**5**	6
$110,000 – $119,999	**6**	4
$120,000 – $129,999	**4**	1
$130,000 – $139,999	**-**	3
$140,000 – $149,999	**4**	1
$150,000 – $159,999	**1**	-
$160,000 – $169,999	**1**	1
$170,000 – $179,999	**2**	1
$190,000 – $199,999	**-**	1
$200,000 – $209,999	**1**	-
$210,000 – $219,999	**-**	2
$220,000 – $229,999	**2**	-
$340,000 – $349,999	**1**	-
$360,000 – $369,999	**-**	1

Commissioner's total remuneration

In accordance with the disclosure requirements of section 152(1)(a) of the Crown Entities Act, the total remuneration, as set independently by the Remuneration Authority, includes all benefits paid during the period 1 July 2025 to 30 June 2026.

Name	Position	Amount 2026	Amount 2025
Michael Webster	Privacy Commissioner	424,079	421,149

Severance payments

Severance payments relate to the termination of employment whether monetary in nature or otherwise. These payments are additional to any final payment of salary, holiday pay or superannuation contributions. For the year ended 30 June 2026, the Office made severance payments to 3 employees totalling $15,610 (30 June 2025: $nil).

Indemnity and insurance disclosures

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

EEO profile

Our human resource policies and programmes are aligned to and consistent with our EEO Policy, as outlined in our Statement of Intent 2023-2027. In addition, we have policies in place to address employee professional development needs, harassment prevention, as well as health, safety and employee wellbeing.

As a member of Te Uru Tāngata Centre for Workplace Inclusion (previously named Diversity Works New Zealand), we seek to follow good practice in key areas such as recruitment and career development to ensure we attract and retain the talent we need to deliver on our ambitious work programmes. We have support also from our Health, Safety and Wellbeing Committee, made up of staff across the organisation. This group is actively involved in developing new initiatives to respond to areas of need with a strong focus on employee wellbeing and resilience.

In the previous year, we updated our Kia Toipoto Action Plan to address pay inequities – particularly for Māori, Pacific, other ethnic pay groups, and members of the Rainbow and disability communities. This supports our commitment of ensuring fair workplace practices and delivering a diverse and inclusive workplace.

Workplace FTE profile – as at 30 June 2026

Role	Full-time	Part-time	Fixed-term	Total
Commissioner	1	-	-	**1.0**
Deputy Commissioner	1	-	-	**1.0**
Senior managers	2	-	-	**2.0**
Team and unit managers	7	-	0.8	**7.8**
Investigations and Dispute Resolution	7	0.7	-	**7.7**
Administrative support	3	0.8	-	**3.8**
Policy	4	0.8	-	**4.8**
Compliance and Enforcement	6	-	-	**6.0**
Capability and Guidance	2	-	1.0	**3.0**
Strategy, Insights and Communications	1	2.2	-	**3.2**
Legal	2	0.9	-	**2.9**
Total	**36**	**5.4**	**1.8**	**43.2**

The figures above do not include secondees and contractors.

The figures also do not include employees on parental leave, where these roles have been covered by Fixed-term contracts.

In the prior year, the corresponding table reported headcount.

Finance and performance

Pūrongo whakahaere pūtea me ngā tutukitanga

Statement of performance

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 2023–2027 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 order to achieve the high-level objectives, the Office also identified three strategic priorities for the 2025/26 year as outlined in our Statement of Performance Expectations for the year ended 30 June 2026. These priorities are:

- provide guidance and develop processes to support the implementation of legislative and regulatory privacy initiatives, including our upcoming responsibilities as a regulator under the Customer and Product Data Bill
- engage with agencies to build their privacy capability and empower New Zealanders to assert their privacy rights
- focus our activities on the technological and digital innovations being adopted by organisations and businesses.

A summary of the key work undertaken within each of these areas is also highlighted in the section noted above.

To support the delivery of our strategic focus, we have determined five output class areas (Functions) that contribute to the overall outcome. These are consistent with the previous year and we report our progress against these Functions in this section.

PBE FRS 48 Service Performance Reporting

PBE FRS 48 is the relevant reporting standard and establishes generally accepted accounting practice and high-level requirements for reporting on service performance. This standard has been applied when collating and reporting information for the Service Performance measures for the year ended 30 June 2026.

As noted above, the Statement of Intent covering the period 1 July 2023 to 30 June 2027 and the Statement of Performance Expectations for the year to 30 June 2026 each set out the longer-term strategy of the Office as well as the specific priorities set for the year to 30 June 2026. The three priorities identified for the 2026 year were established to build upon the major successes we had in 2024/25, including the development of the Biometric Processing Privacy Code, the completion of the Inquiry into Foodstuffs North Island Facial Recognition Trial and issuing of our comprehensive suite of guidance Poupou Matatapu – Doing Privacy Well. During the year, the Office has issued the Biometric Processing Privacy Code, completed a comprehensive suite of guidance relating to children and young people's privacy and initiated the Inquiry into the Cyber Security Breach affecting the Manage My Health Limited Patient Portal.

How the measures were selected

The performance measures have remained consistent with those included in the prior year's Annual Report. There has been some rewording of measures within Communications and Engagement and Compliance and Enforcement functions to better reflect the Office's current environment and fiscal savings.

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 document. The Office considers feedback that it receives and makes changes it thinks are necessary or would improve overall reporting.

Judgements and measurements

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. Targets have been reviewed to focusing on data capturing mechanisms and qualitative characteristics.

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 2026.

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

Statement specifying comprehensive income

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

Specified comprehensive income

	Target $000	Achievement $000
Revenue		
Crown revenue	7,641	7,641
Other revenue	326	210
Total income	**7,967**	**7,851**

The appropriation received by the Privacy Commissioner equals the government's actual expenses incurred in relation to the appropriations, which is a required disclosure under 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 2% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2025/26. The total expenses in the year are $8,714k as set out in the following cost of service statement.

Cost of service statement

for the year ended 30 June 2026

As set out in the 2025/26 Statement of Performance Expectations, the Privacy Commissioner committed to provide five functions. The split of funds across these five functions is set out below:

	Actual 2026 $000	Budget 2026 $000	Actual 2025 $000
FUNCTION 1: Strategy and insights			
Resources employed			
Revenue	920	893	944
Expenditure	1,026	997	989
Net (Deficit)	**(106)**	**(104)**	**(45)**
FUNCTION 2: Communication and Education			
Resources employed			
Revenue	1,272	1,320	1,313
Expenditure	1,375	1,339	1,317
Net (Deficit)	**(103)**	**(19)**	**(4)**
FUNCTION 3: Compliance and Enforcement			
Resources employed			
Revenue	1,741	1,739	1,722
Expenditure	1,968	1,975	1,803
Net (Deficit)	**(227)**	**(236)**	**(81)**
FUNCTION 4: Policy and Advocacy			
Resources employed			
Revenue	1,815	1,857	1,780
Expenditure	1,967	1,991	1,804
Net (Deficit)	**(152)**	**(134)**	**(24)**

	Actual 2026 $000	Budget 2026 $000	Actual 2025 $000
FUNCTION 5: Investigation and dispute resolution			
Resources employed			
Revenue	2,103	2,158	2,075
Expenditure	2,378	2,322	2,174
Net (Deficit)	**(275)**	**(164)**	**(99)**
TOTALS			
Resources employed			
Revenue	7,851	7,967	7,835
Expenditure	8,714	8,624	8,087
Net (Deficit)	**(863)**	**(657)**	**(252)**

The following table 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:

Criteria	Rating
On target or better	Achieved
< 10% away from target	Substantially achieved
>10% away from target	Not achieved

Performance against statements of service performance

for the year ended 30 June 2026

Function 1:
Strategy and Insights

Activity areas of focus

Promoting better prioritisation and decision making through analysis of enquiries, complaints, privacy breaches and other information we receive. Develop and maintain an understanding of the impact of technological developments on privacy. Monitor the success of our strategies and initiatives.

Output Measures

Measure	Estimate	Achieved 2025/2026	Achieved 2024/2025
Conduct 2 assessments a year to gauge the privacy maturity or attitudes of agencies or individuals.	2	**Achieved** During the year we undertook our 2026 survey of New Zealanders covering privacy concerns and data sharing. We also surveyed agencies who had reported to us with a privacy breach or incident (i.e. breach notifying agencies).	**Achieved** During the year we undertook our 2025 survey of New Zealanders covering privacy concerns and data sharing. We also approached a range of agencies who conduct surveys of specific sectors to see if we could include key questions relating to gauging the privacy understanding of agencies. We then undertook a short survey through the Institute of Directors asking these questions.

Function 2:
Communications and Education

Activity areas of focus

Informing people about their privacy rights. Promoting privacy understanding and competence, using media, opinion writing, events and conferences, and stakeholder engagement. Producing material and resources to inform, guide and educate.

Output Measures

Measure	Estimate	Achieved 2025/2026	Achieved 2024/2025
Education module completions as a percentage of education module registrations in the year.	75%	**Achieved – 83%**[11]	**Achieved – 82%**
Respond to all public enquiries within 5 working days.	95%	**Not achieved – 68%** This target only covers to April 2026 – see footnote.[12]	**Substantially achieved – 90%**
Content improvements made to digital service channels.	Achieved	**Achieved** The website redevelopment project and upgrade was completed during the year using in-house resource.	**Achieved** During 2024/25 our focus has been on condensing and improving the presentation and plain language on a range of pages on our website. We developed a new organisational 'look and feel' for OPC and front page for our website, to make key information more easily findable.

11. This calculation is based on total completions during the year as a percentage of total registrations during the year. There may be a small number of completions where registration took place in a prior year. This is consistent with the approach for previous years.
12. For many years we have operated a bespoke enquiries service. The volume of these has long outnumbered our ability to answer them. Many can also be answered by our website. For this reason, on 31 March 2026 our enquiries email address was closed. On 1 May our phone number changed to be a menu of self-help options. The measurement of this KPI therefore ended on the 30 April.

Function 3:
Compliance and Enforcement

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, and enforcement of policy work to ensure compliance.

Output Measures

Measure	Estimate	Achieved 2025/2026	Achieved 2024/2025
Notified privacy breaches that are likely to cause serious harm, are followed up with the notifying agency within 10 working days of risk assessment.	85%	**Achieved – 99.8%** 1,706 out of 1,710 were followed up.	**Achieved – 95%**
The percentage of externally reviewed compliance investigations that are rated as 3.5 out of 5 or better for quality.	85%	**Achieved – 100%** The review was undertaken by an external consulting firm. The result is based on a review of a sample of 6 compliance investigations. The average score for the files reviewed was “4.3 out of 5”. 100% of the files were rated 4.0 or higher.	**Achieved – 100%** The review was undertaken by an external consulting firm. The result is based on a review of compliance notices and compliance investigations.
Incoming compliance issues are risk assessed on allocation to determine the appropriate response activity.	90%	**Achieved – 99.8%** 2,167 out of 2,172 files were risk assessed.	**Achieved – 99%**

Function 4:
Policy and Advocacy

Activity areas of focus

Developing interventions such as guidance and Codes of Practice so that our expectations as a regulator are clear. Provide advice on the primary implications of policies being developed by Government. Advocate for privacy positive outcomes.

Output Measures

Measure	Estimate	Achieved 2025/2026	Achieved 2024/2025
The percentage of externally reviewed policy files that are rated as 3.5 out of 5 or better for quality.	85%	**Achieved – 93%** The review was undertaken by an external consulting firm and the result is based on a review of a sample of 15 files selected by the reviewer. Criteria are set out below.[13]	**Achieved – 93%**
Undertake 2 projects relevant to setting privacy standards, expectations or guidance in the privacy system.	Achieved	**Achieved** Amended the Telecommunications Information Privacy Code 2020 to better support the sharing of location information. Supported the new indirect notification principle in the Act with guidance, privacy code amendments, and sector specific guidance.	**Achieved** Completed the Inquiry into Foodstuffs North Island trial use of Facial Recognition Technology. Completed the development of the Biometric Processing Privacy Code (issued in August 2025). Developed guidance to help implement the new indirect notification principle that will be introduced by the Privacy Amendment Bill.
All externally reviewed policy files appropriately incorporate Treaty and te ao Māori analysis as necessary.	85%	**Achieved – 88%** The reviewer noted that while there was limited consideration of te ao Māori perspectives and Treaty of Waitangi, where te ao Māori perspectives were covered, the work was well done.	**Achieved** The reviewer noted that while there was limited consideration of te ao Māori perspectives and Treaty of Waitangi, where te ao Māori perspectives were covered, the work was well done.

13. 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 outstanding. An overall average score was calculated across all files reviewed and this was based on the judgement of the reviewer.

Function 5:
Investigations and Dispute Resolution

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 to consider bringing to the Human Rights Review Tribunal.

Output Measures

Measure	Estimate	Achieved 2025/2026	Achieved 2024/2025
The percentage of notified complaint files closed by settlement between the parties.	50%	**Not achieved – 44%** Not all complaints are amenable to or require settlement to achieve resolution, including because there was not a breach of the Act. This is one of the reasons why we have moved away from this KPI for 2026/27.	**Achieved – 67%**
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.	85%	**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 selected by the reviewer. The average score for the files reviewed was “4.0 out of 5”. 100% of the files were rated 3.7 or higher.	**Substantially achieved – 80%** The review was undertaken by a Barrister external to the Office and the result is based on a review of a sample of 20 files closed in the year selected by the reviewer. The average score for the files reviewed was “3.6 out of 5”. 100% of the files were rated 3.1 or higher, 80% of the files were rated 3.5 or higher.
The percentage of complaints closed during the year that were less than 6 months old at closure.	85%	**Not achieved – 40%** A complaint file closed in April 2026 was first received in November 2024. This was a representative file constituting 1,672 individual complaints. If this file were excluded from the figures, the percentage of complaints closed during the year less than 6 months old at closure sits at 85%.	**Achieved – 88%** There were 1,221 "Fast Resolve" complaints included in the calculation of this measure, of this 1,215 were resolved in less than 6 months.

Statement of accounting policies

for the year ended 30 June 2026

Reporting entity

These are the financial statements of the Privacy Commissioner, a Crown entity in terms of the Public Finance Act and the Crown Entities Act. 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.

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 2026 and were approved by the Commissioner on 30 October 2026. 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, 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 $33m 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.

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.

Judgements in applying the Privacy Commissioner's accounting policies

Management has exercised the following judgements in applying the Privacy Commissioner's accounting policies for the period ended 30 June 2026:

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

Statement of comprehensive revenue and expenses

for the year ended 30 June 2026

	Note	Actual 2026 $000	Budget 2026 $000	Actual 2025 $000
Revenue				
Crown revenue		7,641	7,641	7,640
Other revenue	2	210	326	195
Total income		**7,851**	**7,967**	**7,835**
Expenditure				
Promotion	4	77	66	116
Audit fees	4	59	55	57
Depreciation and amortisation	4,8,9	83	96	99
Rental expense	4	546	544	557
Operating expenses	4	1,017	1,173	1,029
Contract services	4	271	118	309
Staff expenses	3	6,661	6,572	5,920
Total expenditure		**8,714**	**8,624**	**8,087**
(Deficit)		**(863)**	**(657)**	**(252)**
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		**(863)**	**(657)**	**(252)**

Statement of changes in equity

for the year ended 30 June 2026

	Note	Actual 2026 $000	Budget 2026 $000	Actual 2025 $000
Public Equity as at 1 July		2,189	2,068	2,441
Total comprehensive (deficit)		(863)	(657)	(252)
Public equity as at 30 June	**5**	**1,326**	**1,411**	**2,189**

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

for the year ended 30 June 2026

	Note	Actual 2026 $000	Budget 2026 $000	Actual 2025 $000
Public Equity				
General funds	5	1,326	1,411	2,189
Total public equity		**1,326**	**1,411**	**2,189**
Current assets				
Cash and cash equivalents	6	1,716	1,473	2,271
Receivables (GST)	7	55	28	64
Prepayments	7	121	125	127
Total current assets		**1,892**	**1,626**	**2,462**
Non-current assets				
Property, plant and equipment	8	80	124	134
Intangible assets	9	2	12	4
Total non-current assets		**82**	**136**	**138**
Total assets		**1,974**	**1,762**	**2,600**
Current liabilities				
Payables	10	154	125	194
Employee entitlements	12	344	210	217
Unearned income	2	141	-	-
Total current liabilities		**639**	**335**	**411**
Non-current liabilities				
Lease incentive – non current	11	9	16	-
Total non-current liabilities		9	16	-
Total liabilities		**648**	**351**	**411**
Net assets		**1,326**	**1,411**	**2,189**

Explanations of major variances are provided in Note 1.

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

Statement of cash flows

for the year ended 30 June 2026

	Note	Actual 2026 $000	Budget 2026 $000	Actual 2025 $000
CASH FLOWS FROM OPERATING ACTIVITIES				
Cash was provided from:				
Receipts from the Crown		7,641	7,641	7,640
Receipts from other revenue		326	296	116
Interest received		24	30	79
		7,991	**7,967**	**7,835**
Cash was applied to:				
Payment to suppliers		1,952	1,976	2,156
Payments to employees		6,576	6,582	5,973
Net Goods and services tax (GST)		(9)	(37)	(3)
		8,519	**8,521**	**8,126**
Net cash flows from operating activities		**(528)**	**(554)**	**(291)**
CASH FLOWS FROM INVESTING ACTIVITIES				
Cash was applied to:				
Purchase of property, plant and equipment and intangibles		27	80	12
Cash was provided from:				
Sale of property, plant and equipment and intangibles		-	-	-
Net cash flows from investing activities		**(27)**	**(80)**	**(12)**
Net (decrease) in cash held		(555)	(634)	(303)
Plus opening cash		2,271	2,107	2,574
Closing cash balance	6	**1,716**	**1,473**	**2,271**
Cash held at bank		**1,716**	**1,473**	**2,271**

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

for the year ended 30 June 2026

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 a deficit higher than the budgeted by $206k. This is primarily due to the following:

Other revenue (down on budget by $116k)

$180k has been received from the Ministry of Business, Innovation & Employment to fund work performed in relation to the Customer and Product Data Act 2025. Only $39k has been recognised as income in the year 2025–26 (2024–25 $nil). This is, in part, due to a delay in signing of the Memorandum of Understanding and Funding agreement, and an impact on the work undertaken.

Staff expenses (up on budget by $89k)

There has been an increase in the annual leave accrual of $104k. Lower salary costs due to vacancies have been countered by increased costs for incoming secondees.

Contract services (up on budget by $153k)

The main increase against budget is due to the Office engaging contractors to assist with the Manage My Health Inquiry.

Other operating expenses (down on budget by $156k)

The underspend was due to cost reduction in various areas, most notably staff development and computer maintenance and network costs.

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 and income

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.

At 30 June 2026, there is $141k in Unearned income (2025 $nil) for work to be performed in relation to the Customer and Product Data Act 2025.

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.

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 (2025: $nil).

Other revenue breakdown

	Actual 2026 $000	Actual 2025 $000
Other grants received	116	116
Other revenue	70	-
Interest revenue	24	79
Total other revenue	**210**	**195**

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 2026 $000	Actual 2025 $000
Salaries and wages	6,045	5,569
Employer contributions to defined contribution plans	214	193
Other staff expenses	275	211
Increase/(decrease) in employee entitlements	127	(53)
Total staff expenses	**6,661**	**5,920**

The figures above show temporary staff and secondments as part of Other staff expenses.

This is a change of approach from previous years (where it formed part of Salaries and wages).

The figures for 2025 have therefore been restated accordingly.

Note 4: Other expenses

Accounting policy

Operating leases

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

Judgements in applying accounting policies

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 2026 $000	Actual 2025 $000
Fees paid to auditors:		
External audit	59	57
Promotions costs:		
Website expenses	58	100
Privacy Week/Forum	4	3
Other marketing expenses	15	13
Total promotion expenses	**77**	**116**
Depreciation and amortisation:		
Furniture and fittings	51	57
Computer and equipment	23	32
Office equipment	7	6
Intangibles	2	4
Total depreciation and amortisation	**83**	**99**
Rental expense on operating leases	546	557
Contract services	271	309
Other operating expenses:		
Computer maintenance/ licences	302	277
Staff travel	61	67
Staff development	34	57
Recruitment	9	22
Utilities	304	328
Other	307	278
Total other operating expenses	**1,017**	**1,029**

Operating leases as lessee

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

	Actual 2026 $000	Actual 2025 $000
Not later than one year	357	537
Later than one year and not later than five years	1,891	595
Later than five years	670	-
Total non-cancellable operating leases	**2,918**	**1,132**

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The Wellington lease has been renewed to December 2032, with two subsequent rights of renewal. The Wellington lease will finally expire in December 2038. The Auckland lease will expire in November 2028.

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

A lease incentive has also been offered for the Wellington lease renewal. This takes effect from January 2027.

In April 2024, the Privacy Commissioner entered into a lease agreement for the lease of its printers. The term is 60 months ending April 2029.

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 2026 $000	Actual 2025 $000
Opening balance	2,189	2,441
Net (deficit)	(863)	(252)
Closing balance	**1,326**	**2,189**

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 2026 $000	Actual 2025 $000
Cash on hand and at bank	526	110
Cash equivalents – on call accounts	1,190	2,161
Total cash and cash equivalents	**1,716**	**2,271**

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 fair value, less an allowance for expected losses.

	Actual 2026 $000	Actual 2025 $000
Receivables	55	64
Prepayments	121	127
Total	**176**	**191**
Total receivables comprises		
GST receivable (exchange transaction)	55	64
Total	**55**	**64**

The carrying value of receivables approximates their fair value.

Note 8: Property, plant and equipment and further information

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.

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.

	Furniture and fittings $000	Computer equipment $000	Office equipment $000	Total $000
Cost				
Balance at 1 July 2024	324	195	61	580
Additions	-	6	-	6
Disposals	-	(14)	(5)	(19)
Balance at 30 June 2025	**324**	**187**	**56**	**567**
Additions	3	16	8	27
Disposals	-	-	-	-
Balance at 30 June 2026	**327**	**203**	**64**	**594**
Accumulated depreciation				
Balance at 1 July 2024	168	143	46	357
Depreciation expense	57	32	6	95
Elimination on disposal	-	(14)	(5)	(19)
Balance at 30 June 2025	**225**	**161**	**47**	**433**
Depreciation expense	51	23	7	81
Elimination on disposal	-	-	-	-
Balance at 30 June 2026	**276**	**184**	**54**	**514**
Carrying amounts				
At 1 July 2025	**99**	**26**	**9**	**134**
At 30 June 2026	**51**	**19**	**10**	**80**

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 2026. (2025: $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.

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, and 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

The IASB's Interpretation Committee issued an agenda decision in April 2021 that clarified the accounting treatment expected under the International Financial Reporting Standards for customisation and configuration costs associated with software as a service (SAAS) arrangements.

Where software is provided under a Software-as-a-service (SaaS) arrangement, costs of configuration and customisation are recognised as an intangible asset only if the activities create an intangible asset that Privacy Commissioner controls and asset recognition criteria are met. Costs, including ongoing fees for use of software, that do not result in an intangible asset or a software finance lease are expensed as a service contract as incurred. However, where fees represent payment for future services to be received, Privacy Commissioner recognises these as a prepayment and expenses these as subsequent services are received.

Staff training costs are recognised as an expense when incurred.

There have been $nil software capitalisations in the year to 30 June 2026 (2025: $6k).

	Acquired software $000	Interactive tools $000	Total $000
Cost			
Balance at 1 July 2024	92	652	744
Additions	-	6	6
Disposals	(19)	-	(19)
Balance at 30 June 2025	**73**	**658**	**731**
Additions	-	-	-
Disposals	-	-	-
Balance at 30 June 2026	**73**	**658**	**731**
Accumulated depreciation			
Balance at 1 July 2024	92	650	742
Depreciation expense	-	4	4
Elimination on disposal	(19)	-	(19)
Balance at 30 June 2025	**73**	**654**	**727**
Depreciation expense	-	2	2
Elimination on disposal	-	-	-
Balance at 30 June 2026	**73**	**656**	**729**
Carrying amounts			
At 1 July 2025	**-**	**4**	**4**
At 30 June 2026	**-**	**2**	**2**

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 2026. (2025: $nil).

Note 10: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

	Actual 2026 $000	Actual 2025 $000
Payables under exchange transactions		
Creditors	38	100
Accrued expenses	109	91
Lease incentive	7	3
Total Payables under exchange transactions	**154**	**194**
Total creditors and other payables	**154**	**194**

There were no payables under non-exchange transactions (2025 $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 2026 $000	Actual 2025 $000
Lease incentive	9	-
Total non-current liabilities	**9**	**-**

Lease incentive for the Auckland office for the period 1 December 2025 to 30 November 2028 (3-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.

	Actual 2026 $000	Actual 2025 $000
Current employee entitlements are represented by:		
Accrued salaries and wages	45	22
Annual leave	299	195
Total employee entitlement	**344**	**217**
Current	344	217
Non-current	-	-
Total employee entitlements	**344**	**217**

Note 13: Contingencies

There are no known contingencies existing at balance date (2025: $nil).

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.

	Actual 2026 $000	Actual 2025 $000
Key management personnel compensation		
Total Salaries and other short-term employee benefits	1,224	1,201
Full-time equivalent members	4.0	4.0

Note 15: Post balance date events

Subsequent to 30 June 2026, the Office announced a proposed restructuring. At the date these financial statements were authorised for issue, consultation with affected employees was ongoing and no final decisions regarding the structure, staffing impacts, or implementation arrangements had been made. The proposal is considered a non-adjusting event under PBE IPSAS 14, and as a result no provision has been recognised in these financial statements. The financial impact of the proposal cannot yet be reliably estimated.

Note 16: Financial instruments

Financial instrument categories

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

	Actual 2026 $000	Actual 2025 $000
FINANCIAL ASSETS		
Financial assets measured at amortised cost		
Cash and cash equivalents	1,716	2,271
Receivables (excluding prepayments and taxes receivable)	-	-
Total financial assets	**1,716**	**2,271**
FINANCIAL LIABILITIES		
Financial liabilities measured at amortised costs		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	147	191
Total financial liabilities	**147**	**191**

The Audit Office
Te Mana Arotake

Appendix | Ngā Tāpiritanga

Independent Auditor's Report

To the readers of the Privacy Commissioner's financial statements and performance information for the year ended 30 June 2026

The Auditor-General is the auditor of the Privacy Commissioner. The Auditor-General has appointed me, Bryce Henderson, using the staff and resources of Deloitte Limited, to carry out the audit of the financial statements and performance information on his behalf.

Opinion

We have audited:

- the financial statements of the Privacy Commissioner that comprise the statement of financial position as at 30 June 2026, 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 that include accounting policies and other explanatory information on pages 57 to 72; and
- the performance information that consists of the statement of performance for the year ended 30 June 2026 on pages 47 to 56 and the end-of-year performance information for the appropriations for the year ended 30 June 2026 on pages 52 to 56.

In our opinion:

- The financial statements of the Privacy Commissioner present fairly, in all material respects, its financial position as at 30 June 2026, and its financial performance and cash flows for the year then ended, in accordance with the Public Benefit Entity Standards Reduced Disclosure Regime.
- The performance information is appropriate and meaningful and prepared in accordance with the Privacy Commissioner's measurement bases or evaluation methods and Public Benefit Entity Standards Reduced Disclosure Regime, and presents fairly, in all material respects:
    - the Privacy Commissioner's service performance and actual revenue and expenses for each reportable class of outputs for the year ended 30 June 2026 compared to the forecast standards and budgets included in the statement of performance expectations for the year, and
    - what has been achieved with the appropriation, and the actual expenses or capital expenditure incurred in relation to the appropriation for the year ended 30 June 2026.

The Audit Office
Te Mana Arotake

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, the International Standards on Auditing (New Zealand), and New Zealand Auditing Standard 1 (Revised): *The Audit of Service Performance Information* 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 on behalf of the Privacy Commissioner for preparing financial statements and performance information that are fairly presented and comply with the Public Benefit Entity Standards Reduced Disclosure Regime. This includes:

- the selection of elements/aspects of service performance, performance measures and/or descriptions, and measurement bases or evaluation methods to enable the presentation of service performance information that is appropriate and meaningful; and

- the preparation of a statement of performance, in accordance with the Privacy Commissioner's measurement bases or evaluation methods, that provides an appropriate and meaningful basis to enable readers to assess what has been achieved for the year.

The Privacy Commissioner is also responsible for the preparation of end-of-year performance information for an appropriation that is prepared in accordance with the entity's measurement bases or evaluation methods and complies with the Public Benefit Entity Standards Reduced Disclosure Regime and legislative requirements.

The Privacy Commissioner is responsible for such internal control as they determine is necessary to enable them 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 performance information, the Privacy Commissioner is responsible on behalf of the Privacy Commissioner 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.

The Audit Office
Te Mana Arotake

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 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 the financial statements and 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 or to the Estimates of Appropriations for the Government of New Zealand for the year ending 30 June 2026.

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 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 obtain an understanding of the process applied by the Privacy Commissioner to select its elements/aspects of service performance, performance measures and/or descriptions and the measurement bases or evaluation methods.

- We evaluate whether:

    - the selection of elements/aspects of service performance, performance measures and/or descriptions and measurement bases or evaluation methods present an appropriate and meaningful assessment of the entity's service performance; and

- the performance information is prepared in accordance with the Privacy Commissioner's measurement bases or evaluation methods, and presents fairly, in all material respects in accordance with the Public Benefit Entity Standards Reduced Disclosure Regime, what has been achieved with the appropriation, and for each class of reportable outputs;
    - the actual performance of the Privacy Commissioner as compared with the forecast standards of performance included in the Privacy Commissioner's statement of performance expectations for the financial year; and
    - the actual revenue earned and output expenses incurred as compared to the expected revenues and the proposed output expenses included in the Privacy Commissioner's statement of performance expectations for the financial year.

- 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 information we audited 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 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 all of the information included in the annual report, but does not include the financial statements, the performance information consisting of the statement of performance and the end-of-year performance information for appropriations, 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

The Audit Office
Te Mana Arotake

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 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)* as applicable for audits of public interest entities 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.



Bryce Henderson
Deloitte Limited
On behalf of the Auditor-General
Auckland, New Zealand
30 October 2026





Privacy Commissioner
Te Mana Mātāpono Matatapu

ISSN 1179-9838 (Print)
ISSN 1179-9846 (Online)