Privacy Commissioner
Te Mana Mātāpono Matatapu

COMPLIANCE NOTICE

Issued under section 123 of the Privacy Act 2020

Agency	Oranga Tamariki - Ministry for Children[1]
Notice number	CN 01/2025a
Means of service	Email

Authority of the Privacy Commissioner to issue compliance notice

1 I am authorised to issue a compliance notice to an agency under Part 6(2) of the Privacy Act 2020 ('Act') if I consider the agency has breached the Act.

2 I have provided Oranga Tamariki with a reasonable opportunity to comment on a written notice pursuant to section 124(3) of the Act.

Compliance notice issued

3 I have determined Oranga Tamariki failed to comply with the requirements of information privacy principle ('IPP') 5 (storage and security of personal information) and IPP 11 (limits on disclosure of personal information) at section 22 of the Act. I consider there is a high likelihood of continuing breaches of IPP 5 and IPP 11.

4 Due to the above I now issue this compliance notice under section 123 of the Act. Oranga Tamariki is required to take the steps set out at paragraph 20(a) to (d) of this notice within the timeframes set out at paragraphs 21, 22 and 23 of this notice to remedy its noncompliance with the Act.

Oranga Tamariki's noncompliance

Background

5 A privacy breach includes unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information held by an agency. A privacy breach becomes notifiable to my Office where it is reasonable to believe it has or is likely to cause serious harm to an affected individual or individuals.

---

[1] Oranga Tamariki / Ministry for Children, A New Zealand government department with duties under the Oranga Tamariki Act 1989.

6 My Office has been engaging with Oranga Tamariki in response to repeated notifiable privacy breach reports made under Part 6(1) of the Act. These reports raised concerns around Oranga Tamariki's storage and security of personal information and unauthorised disclosure of personal information.

7 On 12 December 2022 my office initiated a compliance investigation into Oranga Tamariki's privacy practices. In the context of this investigation, the Deputy Privacy Commissioner wrote to the then Chief Executive of Oranga Tamariki on 12 May 2023 recommending that Oranga Tamariki engage a professional reviewer to carry out an extensive independent assessment over its privacy practice. In response to this recommendation, Oranga Tamariki engaged an external reviewer to carry out a comprehensive assessment of its privacy practice and culture ('the independent review').

8 The report from the reviewer was provided to Oranga Tamariki in April 2024 and shared with my Office. The report identified significant systemic issues which are likely to give rise to ongoing breaches of privacy. The issues identified included:

i. Lack of consideration of privacy / low maturity privacy culture

ii. Lack of operational and IT system control to manage access to sensitive personal information

iii. Lack of reporting, accountability or oversight of privacy breaches and near misses

iv. Lack of oversight and assurance on third party providers / non-Oranga Tamariki staff.

9 The recommendations from the report led to the development of a Privacy Improvement Plan ('PIP') which Oranga Tamariki shared with my Office and expressed commitment to delivering. The PIP focuses on the following areas to uplift Oranga Tamariki's privacy practice and culture:

i. Leadership

ii. Privacy Functions

iii. Skills and capability

iv. Appropriate access

v. Reporting

vi. Assurance

10 I consider that timely completion of the PIP actions is critical to ensure that Oranga Tamariki's governance and management of personal information is fit for purpose.

11 To ensure that the ongoing delivery of the PIP will be effective in addressing the causes of the privacy breaches, I consider it is necessary to issue a compliance notice under Part 6(2) of the Act.

Description of identified noncompliance (section 125(1)(b))

12 From my Office's review of the notifiable privacy breaches, and the outcome of the independent review, I have determined that Oranga Tamariki has not complied with the requirements of IPP 5 (storage and security of personal information) and IPP 11 (limits on disclosure of personal information) at section 22 of the Act.

IPP 5

13 I have identified incidents of:

i. loss of documents and devices containing personal information

ii. unsecured disposal of physical documentation containing personal information

iii. inadequate access controls to systems where personal information is stored

iv. unauthorised staff access to personal information

v. unauthorised duplication of files containing personal information.

14 IPP 5 requires Oranga Tamariki to ensure the personal information it holds is protected by such security safeguards as are reasonable in the circumstances to take against loss, accidental or unauthorised access, use, modification or disclosure, or any other misuse.

15 I do not consider that Oranga Tamariki has taken all necessary steps to ensure that the personal information it holds is protected by all reasonable security safeguards. This lack of reasonable security safeguards is a breach of IPP 5.

IPP 11

16 I have also identified incidents of unauthorised disclosure of personal information, including personal information sent in error to incorrect recipient(s) and failures to unredacted personal information from documents otherwise shared in compliance with the Act.

17 IPP 11 requires that Oranga Tamariki not disclose personal information unless if for or directly connected to the purpose for which it was obtained, or to the person concerned, or when authorised by the person concerned. It may also disclose personal information when it is to be used in a way that does not identify the person concerned, or when the disclosure is necessary to avoid endangering public health or safety or the life or health of an individual, or when the disclosure is necessary to uphold or enforce the law. It may also disclose personal information it has collected from public sources if it would not be unfair or unreasonable in the circumstances.

18 I do not consider that Oranga Tamariki had a reasonable belief that disclosure of the personal information disclosed in error met any of the permitted exceptions. This lack of a reasonable belief that an exception applies is a breach of IPP 11.

Decision to issue compliance notice

Factors set out in section 124(1)

19 Before issuing a compliance notice to an agency, I must consider the factors set out in section 124(1) of the Act to the extent that they are relevant, and to the extent information about the factors is readily available.

20 My reasoning based on the factors set out in section 124(1) of the Act is set out as follows:

i. **Whether there is another means under the Act or another Act for dealing with the breach (124(1)(a))**

I have identified Oranga Tamariki's noncompliance after having assessed the nature and cause of the privacy breaches reported to my Office, and the outcome of the independent review. While Oranga Tamariki has established a PIP and privacy uplift is underway, I consider this notice is necessary to underpin the success of the privacy uplift intended and to remedy the recurring breaches of IPP 5 and IPP 11.

ii. The seriousness of the breaches and ongoing risk (124(1)(b); 124(1)(c); 124(1)(d)

I consider that the notifiable privacy breaches reported to my Office and the systemic issues identified by the independent review to be significant. This is because the sensitivity of the personal information involved and the vulnerability of the individuals that the information relates to is at the high end of seriousness. The breaches demonstrate that Oranga Tamariki currently does not have sufficiently robust systems and practices in place to appropriately protect the personal information it holds as required by the IPPs and there is ongoing likelihood of further privacy breaches.

The privacy breaches demonstrate low privacy maturity within Oranga Tamariki with privacy risks often not able to be identified or mitigated. Prompt identification of notifiable privacy breaches is essential for prompt reporting to my Office as soon as reasonably practicable, under section 114 of the Act. The serious privacy breach incidents that have been notified to my Office have caused significant harm to children and their whanau.

Since the Act became effective in December 2020, my Office has received repeated privacy breach notifications from Oranga Tamariki, of which more than half are notifiable privacy breaches and, in some cases, involved extreme harm. These incidents have put vulnerable children, parents and caregivers at risk as well as retraumatised victims. I consider there is a high and ongoing risk that without taking steps to mitigate the risk, serious privacy breach incidents will continue to occur.

While implementation of the PIP will help to support improved compliance with the IPPs, the specific actions set out in this compliance notice are necessary to address the ongoing risk of further serious privacy breaches resulting in harm to individuals.

iii. Whether the Agency has been co-operative in all dealings with my Office (124(1)(e))

Oranga Tamariki has engaged productively with my Office by accepting the recommendation to commission and independent review and to develop a PIP to implement its recommendations. Oranga Tamariki has also incorporated feedback

from my Office on the PIP. Oranga Tamariki has expressed a commitment to privacy uplift and delivering the PIP.

While we have no doubt the department's leadership is committed to privacy uplift, in the past organisational and personnel changes, and the need to respond to other priorities, has affected Oranga Tamariki's focus on such uplift. This notice is issued to underpin and embed Oranga Tamariki's current commitment to ensure its success in uplifting privacy practice and culture to ensure that the privacy of individuals is protected.

iv. The likely cost to the Agency of complying with the notice (124(1)(f))

This notice requires Oranga Tamariki to uplift staff privacy skills and capability, strengthen information access settings, strengthen oversight of service providers, and strengthen accountability and reporting of privacy breach incidents to comply with the Act.

The current PIP addresses preliminary work to advance improvements and does not include the costs associated with this Notice's requirements. I recognise Oranga Tamariki will need to incur some cost in complying with the Notice. However, I consider that any likely associated cost for Oranga Tamariki to comply with the Notice to be necessary, considering the evident level of serious and ongoing privacy risk.

21 Oranga Tamariki must now take the identified steps within the specified timeframes to remedy its noncompliance with the Act.

Steps that Oranga Tamariki must take to remedy the breach (sections 125(1)(c) and 125(2)(a))

22 I require Oranga Tamariki to take the following steps to remedy its noncompliance with the Act within the applicable timeframes:

i. **Uplift staff skills and capability**: Oranga Tamariki must:

a. Develop and deliver privacy training for all staff including contractors who are under the direct supervision of Oranga Tamariki. The training must:

1. provide direction on the interaction of the Privacy Act with the Family Violence Act and the Oranga Tamariki Act and its associated regulations

2. be tailored to both back-office enabling staff and frontline social workers

3. be provided to new staff as part of induction and prior to gaining system access to personal information

4. be repeated for all staff at appropriate intervals (e.g., annually), with additional refresher training required for specific groups and/or when privacy incidents occur.

ii. **Strengthen information access settings**. Oranga Tamariki must:

a. Strengthen the business rules for all staff and contractors on access and management of personal information. Specifically:

1. complete an assessment of the levels of sensitivity of all types of personal information held ('Privacy Classification System') which includes a record of the location or system where it is stored

2. develop and deliver business rules for role-based access permissions to personal information

3. develop and implement robust procedures for responding to information disclosure requests which require sensitive redacted information to be handled appropriately and within the required timeframes.

b. Develop and implement a business case for strengthening the technical system settings within CYRAS to ensure the access settings align with, and are constrained to, what is required according to the Privacy Classification System. Specifically:

1. develop and implement technical settings for role-based access permissions to personal information

2. implement an audit log and process for the proactive monitoring of access IT security access controls

3. develop and deliver a proactive monitoring schedule and reporting framework that includes adjusting and removing access as appropriate.

iii. **Strengthen oversight of service providers**. Oranga Tamariki must:

a. Strengthen the agency's oversight of devices provided to non-Oranga Tamariki personnel, by:

1. developing and maintaining an inventory of the allocation and use of devices to non-Oranga Tamariki personnel which also records the information access settings for each person

2. review and strengthen contractual requirements for non-Oranga Tamariki staff, including secure information management and disposal practices and prompt privacy breach reporting requirements.

b. Ensure third party social services providers have appropriate privacy policies and practices in place to ensure the protection of Oranga Tamariki's personal information, by:

1. developing a schedule of regular audits of the privacy policies and practices of those providers to ensure the required privacy standards are maintained.

iv. **Strengthen accountability and reporting of privacy incidents**. Oranga Tamariki must:

a. Develop and deliver a privacy performance reporting framework that includes:

1. progress with the PIP delivery until June 2025, and Oranga Tamariki longer-term responses to the Privacy Review findings post June 2025

2. a documented explicit requirement for all staff and non-Oranga Tamariki personnel with access to Oranga Tamariki personal information to report privacy incidents promptly to the privacy team

3. privacy incidents (breaches and near-miss) occurring, as well as insights and trend analysis

4. completion rates for training uptake by all staff and contractors, aligned to an identified completion target for all personnel

5. implementation of controls and recommendations identified in Privacy Impact Assessments

6. the effectiveness of the information access control settings.

Timeframes and reporting (section 125(2)(c))

23. Oranga Tamariki is required to take the steps required in paragraph 22 as follows:

i. Uplift staff skills and capability. Oranga Tamariki must:		
a. Develop and deliver privacy training for all site/region-based staff including contractors/third parties who are under the direct supervision of Oranga Tamariki. The training must:		
1.	provide direction to staff on the interaction of the Privacy Act with the Family Violence Act and the Oranga Tamariki Act and its associated regulations.	Due 30 March 2026
2.	be tailored to both back-office enabling staff and frontline social workers.	Due 31 October 2025
3.	be provided to new staff as part of induction and prior to gaining system access to personal information	Due 31 October 2025
4.	be repeated for all staff at appropriate intervals (e.g., annually), with additional refresher training required for specific groups and/or when privacy incidents occur.	Due 31 October 2025
ii. Strengthen information access settings. Oranga Tamariki must:		
a. Strengthen the business rules for all staff on access and management of personal information. Specifically:		
1.	complete an assessment of the levels of sensitivity of all types of personal information held ('Privacy Classification System') which includes a record of the location or system where it is stored	Due 31 October 2025
2.	develop and deliver business rules for role-based access permissions to personal information	Due 31 October 2025
3.	develop and implement robust procedures for responding to information disclosure requests which require sensitive redacted information to be handled appropriately and within the required timeframes	Due 31 October 2025
b. Develop and implement a business case for strengthening the technical system settings within CYRAS to ensure the access settings align with, and are constrained to, what is required according to the Privacy Classification System. Specifically:		
1.	develop and implement technical settings for role-based access permissions to personal information	Due 30 March 2026
2.	implement an audit log and process for the proactive monitoring of access IT security access controls	Due 31 October 2025
3.	develop and deliver a proactive monitoring schedule and reporting framework that includes adjusting and removing access as appropriate.	Due 31 October 2025

iii. Strengthen oversight of service providers. Oranga Tamariki must:		
a. Strengthen the agency's oversight of devices provided to non-Oranga Tamariki personnel, by:		
1.	developing and maintaining an inventory of the allocation and use of devices to non-Oranga Tamariki personnel which also records the information access settings for each person	Due 31 October 2025
2.	review and strengthen contractual requirements for non-Oranga Tamariki staff, including secure information management and disposal practices and prompt privacy breach reporting requirements.	Due 31 October 2025
b. Ensure third party social services providers have appropriate privacy policies and practices in place to ensure the protection of Oranga Tamariki's personal information, by:		
1.	developing a schedule of regular audits of the privacy policies and practices of those providers to ensure the required privacy standards are maintained	Due 30 March 2026
iv. Strengthen accountability and reporting of privacy incidents. Oranga Tamariki must:		
a. Develop and deliver a privacy performance reporting framework that includes		
1.	progress with the PIP delivery until June 2025, and Oranga Tamariki longer-term responses to the Privacy Review findings post June 2025	Due 31 October 2025
2.	a documented explicit requirement for all staff and non-Oranga Tamariki personnel with access to Oranga Tamariki personal information to report privacy incidents promptly to the privacy team	Due 31 October 2025
3.	privacy incidents (breaches and near-miss) occurring, as well as insights and trend analysis	Due 31 October 2025
4.	completion rates for training uptake by all staff and contractors, aligned to an identified completion target for all personnel	Due 31 October 2025
5.	implementation of controls and recommendations identified in Privacy Impact Assessments	Due 31 October 2025
6.	the effectiveness of the information access control settings.	Due 30 March 2026

24. Oranga Tamariki must provide a quarterly report to my Office setting out progress with meeting the requirements of this notice, with the timing of the first report to be agreed with my Office and then provided at the end of the following financial year quarters.

Variation and cancellation

25. If Oranga Tamariki complies with this notice by the specified dates, I may cancel the notice in accordance with section 127 of the Act.

26. If Oranga Tamariki partially complies with this notice by the specified dates, I may vary the notice in accordance with section 127 of the Act.

Enforcement, appeal, and publication

Enforcement (section 130 & section 133)

27. I may bring enforcement proceedings in the Human Rights Review Tribunal if Oranga Tamariki does not comply with this compliance notice.

Appeal (section 125(1)(d))

28. Oranga Tamariki has the right to appeal this compliance notice to the Human Rights Review Tribunal under section 131 of the Act. The appeal can relate to the notice in whole or in part.

29. The Human Rights Review Tribunal may allow an appeal for one of the reasons listed at section 131(3) of the Act. An appeal must be lodged in the Human Rights Review Tribunal within 15 working days from the date of the issue of this notice.

Publication (section 129)

30. I reserve the right to publish details of this compliance notice in accordance with section 129 and section 206(2) of the Act.

Michael Webster
Privacy Commissioner

Dated: 26 May 2025