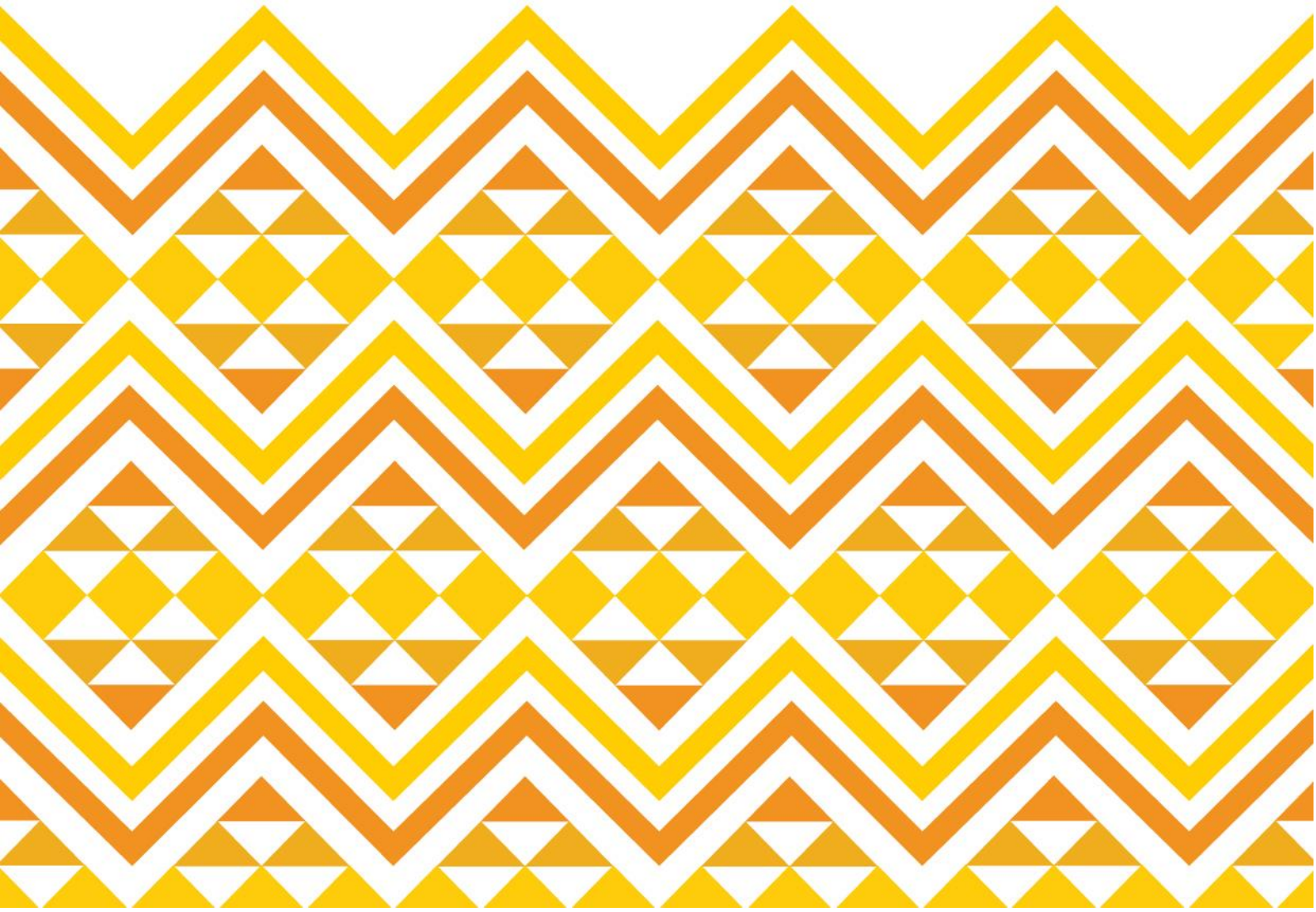
ORANGA TAMARIKI
Ministry for Children

New Zealand Government

Privacy Improvement Plan

1 July 2024 – 30 June 2025



Privacy Improvement Plan – 1 July 2024 – 30 June 2025

Focus Area	Recommendations	Planned Actions
Leadership	Ensure leadership articulates and demonstrates the significance of the personal information we collect and hold, and the responsibilities we all have to not only keep it safe but also to share it where appropriate. Ensure managers and team leaders at all levels understand their privacy obligations and commit their support and assurance.	1. Integrate privacy into the leadership focus and culture reset as part of implementing the new organisational restructure, through: a. Specific communication from the Chief Executive about the Review findings, the Privacy Improvement Plan, and expectations relating to Privacy followed by quarterly messaging from the Chief Executive regarding the importance of privacy considerations in both operations and decision-making. b. All people leaders reinforce this messaging through standing items in team meetings, communications, and initiatives. From a Social Work practice point of view, this will be achieved through the specific and targeted Practice Drop In Sessions, led by the Chief Social Workers Office. *See recommendations in relation to skills and capability for more detail.*
		2. Include explicit accountability and reporting expectations for all people leaders in their annual Performance Expectations, in relation to Privacy, e.g., compliance with the Privacy Act, mandatory completion of Privacy Training, and compliance with the Chief Social Workers Practice Note on Privacy.
		3. Update the Code of Conduct to directly address the confidential and sensitive of information we hold, and the expectations of how it is accessed, used, and handled. Include misuse of personal information as a specific example of misconduct or serious misconduct depending on the severity.
Privacy Functions	Set the Privacy function is at a suitable level within the agency to provide adequate visibility and influence.	4. Place the privacy function in a central group close to practice and delivery.
		5. Elevate the Chief Privacy Officer responsibility from Tier 5 to Tier 2, to signal its importance and give it the weight and visibility required to bring about change.
		6. Identify or create a function responsible for privacy assurance, accountability, and compliance including at the governance level.
Skills and Capability	Ensure our staff understand and are mindful of the significance of the personal information they work with. Ensure new staff working with children and young people receive targeted privacy training during induction and that existing staff have improved understanding of good privacy practice.	7. Implement new step for frontline staff, as part of day 1 induction, requiring direct supervisor to brief new staff member on confidential and sensitive of information we hold, and the expectations of how it is accessed, used, and handled. Investigate how we can prevent access to restricted systems until verification this step has been completed.
		8. Develop Teams based training for all site/region-based staff to reinforce good privacy practices. Training should be appropriate for relational face-to-face practice.
		9. Review current information sharing practice policy and guidance and ensure that this strongly reflects a protection of personal information lens, whilst still maintaining the importance of safe information sharing.
		10. Include a dedicated privacy component in Puāwai training programme as part of the existing legal module. Training should be appropriate for relational face-to-face practice and designed and delivered to achieve the best impact and change in practice and behaviour.
		11. Include a focus on managing privacy in “Leading practice” so this forms part of professional case work supervision.
		12. Develop and roll-out module on privacy breach notification. Design and delivery should be tailored to both back-office enabling staff and frontline social workers.

Focus Area	Recommendations	Planned Actions
Appropriate Access	Commence work to ensure that tamariki, whānau and caregiver information is accessible only to the extent people need it.	13. Prepare and release Chief Social Worker's Practice Note, resetting expectations on privacy. The Practice Note will clarify the interaction of the Privacy Act with the Family Violence Act and the Oranga Tamariki Act and its associated regulations, linking to existing policy and guidance. Monitor change delivered through new reporting mechanisms and insights reported to the Strategy and Risk Governance Group on a quarterly basis. Explore technical ability and resources needed to effectively monitor appropriate access to CYRAS through periodic spot checking and manual review of legitimacy of access.
		14. Rewrite and disseminate the Business Rules regarding access to and management of information. This work will include an assessment of the levels of sensitivity of the various types of information held, being explicit about role-based permissions for accessing information, and the exceptions process. Follow up with education and training through the Practice Drop-In Sessions.
		15. Scope the technical business requirements and the most cost-efficient way to categorise, classify and segregate access to information, including being explicit about role-based permissions for accessing information, in the existing CYRAS systems. Implementation timeframe to be confirmed once requirements and costs are established.
		16. Subject to the findings arising from recommendation 15, implement Privacy Classification System within (constraints of existing) CYRAS system to restrict some roles' access to information in alignment with the criteria developed through recommendation 11.
		17. Scope the business requirements to include new Privacy Classification System within the case record, first tranche of the new Frontline Technology System Upgrade.
Reporting	Make privacy is a key part of performance measurement to learn from missteps.	18. Develop quarterly privacy performance reporting to the Strategy and Risk Governance Group and external Risk and Assurance Committee on: • Progress with Review findings • privacy breaches and near-misses • compliance [training, Practice Note, Performance Expectations], • Implementation of agreed-upon controls and recommendations identified through Privacy Impact Assessments or other Privacy Team review • insights and trend analysis
		19. Document reporting lines and process map for notification of privacy complaints, breaches, and near-misses, and processing of Privacy Act requests for personal information.
Assurance	Make privacy practice a regular part of our assurance cycle.	20. Design appropriate assurance activities to address our ongoing responsibilities and compliance obligations.
		21. Commission a review of progress against the Privacy Improvement Plan.
		22. Develop framework (including timetable for implementation) in collaboration with the Deputy Chief Executive Māori, Partnerships and Communities for rolling out these recommendations across our partners and contracted providers; and to ensure appropriate reporting and monitoring of compliance through existing audit processes, including greater oversight of assignment and use of Oranga Tamariki devices to non-Oranga Tamariki personnel.
		23. Review breach management plan and protocols as needed to ensure consistency as improvements identified in the plan are implemented.